UNIVERSITA' DI PISA

Dipartimento di Economia e Management

Corso di laurea in Economia Aziendale

TESI DI LAUREA

IL SISTEMA DEI CONTROLLI INTERNI NELLE IMPRESE BANCARIE: LA FUNZIONE COMPLIANCE E I RAPPORTI CON LA FUNZIONE DI REVISIONE INTERNA

Candidato

Lorenzo PASSETTI

Relatore

Chiar.ma Prof.ssa Antonella CAPPIELLO

ANNO ACCADEMICO 2012-2013

Indice

Introduzione 6

1 IL SISTEMA DEI CONTROLLI INTERNI 12

1.1 La definizione di controlli interni 12

1.2 Controlli interni, organizzazione aziendale e corporate governance 17

1.3 La struttura del Sistema dei Controlli Interni 21

1.4 L'aspetto funzionale del Sistema dei Controlli Interni 26

1.5 Le componenti del Sistema di Controllo Interno 31

1.6 Le funzioni di controllo interno 34

1.7 La classificazione dei rischi nelle disposizioni di vigilanza di Banca d'Italia 41

2 LA FUNZIONE DI COMPLIANCE 49

2.1 Definizione e funzioni dell'attività di compliance 49

2.2 Il rischio di compliance e la cultura aziendale 56

2.3 I requisiti organizzativi della funzione compliance 65

2.4 La definizione e la quantificazione dei costi di compliance 71

2.5 Il profilo tipico del Compliance officer 77

2.6 La funzione compliance secondo l'approccio di Basilea 78

2.7 Materie rilevanti ai fini della compliance: D.lgs. n. 231/2001 84

2.8 Materie rilevanti ai fini della compliance: Legge MIFID 87

2.9 Materie rilevanti ai fini della compliance: MAD – Market Abuse Directive 92

2.10 Materie rilevanti ai fini della compliance: Antiriciclaggio 94

2.11 Materie rilevanti ai fini della compliance: privacy 99

2.12 Materie rilevanti ai fini della compliance: Antiusura 101

2.13 Materie rilevanti ai fini della compliance: trasparenza delle operazioni e dei servizi bancari 103

3 I RAPPORTI TRA LA FUNZIONE DI COMPLIANCE E LA FUNZIONE DI REVISIONE INTERNA 107

4 LA FUNZIONE DI COMPLIANCE IN BANCA, UN CASO PRATICO: “LA NOSTRA BANCA” 128

4.1 Premessa 128

4.2 Ruolo e compiti della Funzione di Compliance 129

4.3 Ruolo e compiti della Funzione di Revisione Interna 130

4.4 Rapporti tra Compliance e Funzioni Aziendali, con focus sui rapporti con la Revisione Interna 132

5 CONCLUSIONI 140

6 BIBLIOGRAFIA 152

7 WEBSITES 157

Ai miei genitori

Ringraziamenti

Introduzione

Il contesto nel quale operano attualmente gli istituti di credito è caratterizzato da un'elevata e crescente complessità derivante dalle molteplici attività svolte, dai mercati in cui operano, dall'eterogeneità di interlocutori con i quali si relazionano e dal particolare contesto congiunturale che caratterizza la storia dei sistemi economici degli ultimi tre anni.

Ciascuno di questi fattori è interessato da specifiche previsioni normative e regolamentazioni di altra fonte alle quali gli operatori del settore bancario devono necessariamente prestare attenzione.

In conseguenza di ciò, si è registrata negli ultimi tempi un'imponente produzione normativa, sollecitata anche dagli innumerevoli scandali finanziari e dalla conseguente necessità di fornire fiducia e stabilità al sistema di mercato, attraverso una crescente enfasi sulla conformità alle norme e sui comportamenti eticamente corretti, con il principale obiettivo di preservare l'immagine della banca dai rischi di carattere reputazionale.

I cambiamenti regolamentari hanno interessato non solo i mercati domestici ma anche quelli internazionali, con provvedimenti che, inevitabilmente, hanno finito col produrre conseguenze tangibili nell'intero sistema finanziario[1].

La disciplina di mercato che ne è derivata, definita efficacemente come "una sapiente miscela di incentivi e deterrenti, di premi e sanzioni"[2], si caratterizza per la volontà di delimitare l'operato degli intermediari entro i confini di un sistema di norme dirette a regolamentare il mercato, ma al

[1] Per proporre degli esempi è sufficiente citare il Sarbanes Oxley Act, risposta statunitense agli scandali come quelli che hanno coinvolto la Enron e la WorldCom; il Nuovo Accordo di Basilea, che ha rivoluzionato il rapporto banca-impresa; la disciplina degli IAS, che ha uniformato l'informativa di bilancio; la direttiva 2004/39/CE sui servizi d'investimento (MiFID), il cui obiettivo è quello di pervenire ad un mercato finanziario unico europeo.

[2] Comana M. (2005), p.12.

contempo, finalizzata a garantire la necessaria libertà operativa e gestionale delle imprese finanziarie.

Il documento del Comitato di Basilea sull'attività di compliance nelle banche[3], si inquadra perfettamente in tale contesto evolutivo, rappresentando il più rilevante e qualificato contributo al dibattito scaturito nel sistema bancario internazionale sul tema della individuazione dei nuovi modelli per la gestione del rischio di compliance.

Esso introduce nell'organizzazione bancaria una funzione indipendente, destinata all'identificazione, valutazione e al monitoraggio del rischio di non conformità; vale a dire del rischio di incorrere in danni economici e reputazionali, derivanti dalla non conformità a norme, regolamenti o codici di condotta.

L'attività di compliance è considerata una funzione primaria del sistema dei controlli interni, al pari della funzione di risk management e della funzione di revisione interna e viene inserita tra gli strumenti utili al rafforzamento dei presidi di controllo interno alle banche, collocandosi su un piano complementare e funzionale rispetto ai presidi già esistenti.

La nuova disciplina della compliance è, dunque, parte integrante del nuovo quadro dei controlli prudenziali, volto a promuovere il confronto e il dialogo fra banche e autorità di vigilanza, riguardo ai rischi reputazionali e di non conformità e sui presidi patrimoniali e organizzativi ritenuti adeguati a fronteggiarli.

L'adeguamento normativo in materia di conformità, nell'intento di preservare e garantire l'efficienza degli intermediari, tende a contenere i costi della regolamentazione attraverso un approccio, seguito anche dalla Banca d'Italia nel suo documento di consultazione, che enuncia i requisiti

[3] Basel Committee On Banking Supervision (2005).

minimi e riconosce ampia autonomia alle banche nell'organizzazione interna della funzione.

L'orientamento dell'attività di controllo dell'autorità di vigilanza è sempre di più volto a ridurre il peso delle prescrizioni normative e a valorizzare, contestualmente, gli strumenti di supervisione orientati al mercato e incentrati su una crescente responsabilizzazione degli intermediari stessi. Le finalità sottese al controllo prudenziale vanno ravvisate, dunque, nella volontà di "rafforzare il legame tra il profilo di rischio di un intermediario, i suoi sistemi di gestione e di mitigazione dei rischi e il suo capitale"[4].

La nuova disciplina sulla compliance, infatti, accompagna e integra le innovazioni regolamentari in materia di adeguatezza patrimoniale e di rapporti tra supervisor e banche[5]; a queste ultime sarà richiesto di predisporre adeguati processi di definizione del capitale necessario a fronteggiare tutti i rischi a cui sono esposte nell'esercizio della propria attività, compresi i rischi reputazionali e di compliance.

Numerose verifiche empiriche suggeriscono che le politiche di vigilanza più efficaci, nel raggiungimento della stabilità e di elevati livelli di performance, sono quelle che stimolano alla predisposizione di meccanismi di controllo interni[6]. E' evidente, tuttavia, che l'efficacia di tale impostazione, è tanto maggiore quanto più elevato è il livello di concorrenza dei mercati; i comportamenti che da essa derivano favoriscono lo sviluppo di una "cultura del controllo" quale condizione necessaria per una "sana e prudente" gestione aziendale.

[4] CEBS (2006).
[5] Clemente C. (2006).
[6] A tal riguardo Barth, Caprio e Levin hanno dimostrato che quei paesi in cui esistono maggiori restrizioni all'operato delle banche, presentano anche sistemi bancari più fragili e che esiste una correlazione inversa fra le crescenti restrizioni regolamentari e le performance bancarie. Barth J. R., Caprio G., Levine J. (2001b).

La formazione di una "cultura" aziendale orientata al rispetto delle regole e alla creazione di valore diviene, pertanto, un requisito essenziale per garantire la conformità alle norme ai regolamenti e ai codici di condotta interni e, in tal senso, rappresenta un elemento di produzione del valore. Considerando la definizione di attività di compliance, in precedenza proposta, è possibile individuare almeno tre principali direttive di creazione del valore:

1. Per l'intermediario l'accresciuta consapevolezza dei rischi della gestione aziendale permette un controllo più attento delle eventuali perdite monetarie derivanti da multe e sanzioni o di eventuali contrazioni dei ricavi o dei volumi di vendita indotti da una perdita di fiducia della clientela e incide positivamente sui processi di valutazione delle società di rating e sul costo del funding.

2. Per i clienti l'attività di compliance rappresenta un fattore di valorizzazione del rapporto fiduciario alla base dei processi di intermediazione.

3. In un'ottica di tutela della disciplina mercato la funzione di verifica della conformità è un elemento che interferisce positivamente sulla credibilità dei sistemi di mercato.

Come evidente l'attività di controllo sul rischio di non conformità è strettamente legata ai rischi legali e reputazionali; il suo potenziamento può rappresentare per gli intermediari bancari un'occasione utile per recuperare la fiducia da parte degli investitori e limitare i danni economici derivanti dalla non conformità alle leggi e ai regolamenti vigenti.

L'istituzione delle funzioni aziendali preposte alla gestione dei rischi di non conformità diventa una mossa strategica di gestione aziendale, che nasce dalla constatazione di agire in un contesto internazionale integrato e altamente competitivo.

Il rispetto di leggi e regolamenti diviene una componente distintiva, destinata a favorire gli intermediari finanziari in grado di capire e sfruttare a proprio vantaggio il cambiamento in atto. In sintesi, la funzione di compliance rappresenta la risposta gestionale all'aumento della complessità dei rischi dell'attività bancaria in un contesto altamente competitivo come il sistema di mercato e alla consapevolezza che il rispetto delle regole costituisce un fattore di creazione del valore per l'impresa[7], attraverso la prevenzione o la riduzione delle perdite di capitale derivanti da sanzioni, multe o danni reputazionali e attraverso l'impulso allo sviluppo delle relazioni di clientela.

La corporate governance in questo contesto gioca un ruolo fondamentale, intervenendo nell'adeguare l'organizzazione esistente in modo coerente con l'obiettivo di gestire i conflitti d'interesse e ridurre al minimo i comportamenti in contrasto con norme, regolamenti, codici di condotta e best practice e infondendo una cultura della legalità che pervada ogni aspetto dell'attività bancaria. A tal fine, devono essere previste "una chiara definizione dei poteri e delle responsabilità operative e decisionali; un sistema di controllo interno capace di individuare tempestivamente le criticità; un organismo di vigilanza interno, indipendente dagli altri organi aziendali e con autonomi poteri decisionali"[8].

L'attività di compliance è stata introdotta, per la prima volta nel nostro Paese, con il documento di consultazione della Banca d'Italia dell'agosto 2006[9], che rappresentava un primo documento di recepimento degli orientamenti del Comitato di Basilea[10] in materia di conformità alle norme.

Il presente lavoro, rappresentato in questa tesi, è orientato ad analizzare la Funzione di Compliance, il suo ruolo all'interno del sistema dei controlli

[7] Cfr.: Clemente (2006).
[8] Cola C. (2005).
[9] Banca d'Italia (2006).
[10] Basel Committee On Banking Supervision (2005).

interni e i rapporti che la funzione stessa instaura con gli altri attori dell'organigramma aziendale, in special modo la funzione di revisione interna. A tal proposito, a chiusura del lavoro verrà descritto il modello aziendale adottato da un importante player bancario nazionale per la gestione del rischio di non conformità.

Nel dettaglio, nel primo capitolo si vogliono delineare le caratteristiche e le peculiarità del sistema dei controlli interni degli intermediari creditizi, sottolineando l'importanza, nelle dinamiche aziendali, della diffusione della cultura del controllo.

Nel secondo capitolo viene analizzata la Funzione di Compliance, ripercorrendo brevemente le fasi relative alla sua introduzione nell'organismo azienda e dettagliando la sua collocazione aziendale e la mission che gli è stata assegnata.

Nel terzo capitolo viene descritta la Funzione di Revisione Interna e vengono delineati i rapporti che la stessa instaura con la funzione di gestione del rischio di non conformità.

Nel quarto capitolo, al fine di fornire un riscontro pratico all'analisi svolta, viene descritto l'approccio adottato da un importante Banca Nazionale per la gestione del rischio di non conformità.

Infine, il lavoro prevede le considerazioni finali dell'autore.

1 IL SISTEMA DEI CONTROLLI INTERNI

1.1 La definizione di controlli interni

Il Sistema dei Controlli Interni è un concetto relativamente recente del diritto societario nazionale, che in passato contemplava il Collegio Sindacale quale unico soggetto investito del controllo interno all'azienda, con funzioni di sorveglianza sulla correttezza della gestione.

Tuttavia l'evoluzione nelle tecniche di governance e il nuovo orientamento della gestione adottato dagli intermediari bancari improntato alla forte attenzione ai rischi, hanno comportato una maggiore considerazione del controllo interno, sino ad assumerlo come fondamento del buon governo.

Il moltiplicarsi di precetti, frutto della stratificazione dei diversi provvedimenti, non ha però condotto all'individuazione di una definizione univoca in grado di sintetizzare la complessità della materia e – a seconda delle fonti prese in considerazione – vengono valorizzati solo alcuni aspetti del controllo interno.

La prima definizione, quella a cui fare continuo riferimento, è stata fornita dal Committee of Sponsoring Organizations of the Treadway Commission (CoSO) nel 1992 all'interno dell'autorevole documento denominato "CoSO Report", dal quale hanno successivamente preso spunto i regolamenti emanati dal Comitato di Basilea e da Banca d'Italia. La definizione riportata individua il controllo interno quale "processo, svolto dal consiglio di amministrazione, dai dirigenti e da altri operatori della struttura aziendale, che si prefigge di fornire una ragionevole sicurezza sulla realizzazione degli obiettivi di:

- efficacia ed efficienza delle attività operative;
- attendibilità delle informazioni di bilancio;

- conformità alle leggi e ai regolamenti in vigore"[11].

Appare chiaro sin da subito come il controllo interno sia uno strumento al servizio del management per il raggiungimento degli obiettivi prefissati, in grado di fornire la ragionevole certezza della correttezza nella gestione secondo i canoni di efficacia ed efficienza, dell'attendibilità dei dati contenuti nel bilancio quale principale fonte di informazione societarie e dello svolgimento dell'attività conformemente alle normative e ai regolamenti ai quali l'azienda bancaria è sottoposta.

Ispirandosi a quanto indicato dal "Coso Report", il Comitato di Basilea ha fornito una definizione analoga rintracciabile nello "Schema per i sistemi di controllo interno nelle organizzazioni bancarie" pubblicato nel 1998. In esso vengono ripresi i tratti fondamentali già esposti, integrati inoltre dalla precisazione che "esso [il sistema] non consiste unicamente in una procedura o in una politica applicata in un dato momento, bensì opera costantemente a tutti i livelli all'interno della banca. Al consiglio di amministrazione e all'alta direzione compete la responsabilità di instaurare una cultura che favorisca un efficace processo di controllo interno e di sorvegliarne l'efficacia in modo continuativo; tuttavia, a questo processo deve partecipare ogni individuo che opera nell'organizzazione. I principali obiettivi di un sistema di controllo interno possono essere classificati come segue:

- efficienza ed efficacia delle attività (obiettivi di performance);
- affidabilità, completezza e tempestività dei rendiconti finanziari e di gestione (obiettivi di informazione);
- conformità con le leggi e le regolamentazioni applicabili (obiettivi di conformità)".

[11] La definizione riportata è basata sulla traduzione italiana curata da PricewaterhouseCoopers ne "Il sistema di controllo interno. Un modello integrato di riferimento per la gestione dei rischi aziendali", Milano 2004.

In tale rivisitazione della definizione originale è stata sottolineata la stabilità del controllo interno nell'organizzazione, creato per fornire il proprio apporto all'amministrazione[12] in maniera continuativa. Non si tratta dunque di una semplice procedura applicabile meccanicamente per la risoluzione delle criticità. Una sfumatura differente è stata invece enfatizzata nelle "Istruzioni di vigilanza per le banche" pubblicate da Banca d'Italia nel 1999: "*il sistema dei controlli interni è costituito dall'insieme delle regole, delle procedure e delle strutture organizzative che mirano ad assicurare il rispetto delle strategie aziendali e il conseguimento delle seguenti finalità:*

- *efficacia ed efficienza dei processi aziendali (amministrativi, produttivi, distributivi, ecc.);*
- *salvaguardia del valore delle attività e protezione dalle perdite;*
- *affidabilità e integrità delle informazioni contabili e gestionali;*
- *conformità delle operazioni con la legge, la normativa di vigilanza nonché con le politiche,*
- *i piani, i regolamenti e le procedure interne".*

Le successive "*Nuove disposizioni di vigilanza prudenziale per le banche*" (2006) sono intervenute su quanto già esposto precisando che "*al fine di fronteggiare i rischi a cui possono essere esposte, le banche si dotano di idonei dispositivi di governo societario e di adeguati meccanismi di gestione e controllo. Tali presidi si inseriscono nella più generale disciplina dell'organizzazione e del sistema dei controlli interni volta ad assicurare una gestione improntata a canoni di efficienza, efficacia e correttezza".*

[12] Il comitato di Basilea nelle proprie indicazioni cita esplicitamente il consiglio di amministrazione e l'alta direzione, precisando tuttavia come – data la portata generale del provvedimento e l'eterogeneità del pubblico al quale si rivolge – non si faccia riferimento a concetti giuridici, ma l'intento sia quello di indicare attraverso questi le funzioni decisionali degli enti.

Nel testo rinnovato è rintracciabile la forte enfasi che l'Autorità di Vigilanza nazionale ha sottolineato in merito agli aspetti organizzativi che interessano i controlli interni. Inoltre è stata rimarcata l'importanza della preservazione dell'azienda dai rischi connessi all'esercizio della propria attività quali componenti onerose. Si è dunque proseguito nel completamento della direzione indicata dal Comitato in relazione alla stabilità dei controlli interni, incardinandoli all'interno dell'organizzazione aziendale.

In ragione delle definizioni formulate – tutte riconducibili al medesimo concetto di controllo interno nonostante le differenti sfumature che le contraddistinguono – è possibile notare come il controllo di origine anglosassone assuma una connotazione del tutto difforme da quella comunemente utilizzata. È lontana l'idea delle verifiche ispettive e burocratiche, finalizzate all'accertamento dei disallineamenti normativi e al riscontro delle inefficienze gestionali basate su riscontri successivi.

I controlli che si svolgono internamente all'attività aziendale hanno lo scopo di indirizzare la corretta gestione attraverso un'attività di supporto che permetta il raggiungimento dei risultati prospettati.

Così come il management fissa la soglia di performance ritenuta soddisfacente (Risk Appetite) e si avvale della Direzione per il concreto raggiungimento degli obiettivi, altrettanto compie il controllo interno fornendo il proprio contributo alla realizzazione dei piani aziendali.

Si tratta di una visione innovativa, lungi dall'approcciarsi all'attività attraverso un atteggiamento passivo e rigidamente formalizzato nel proprio ruolo: il controllo prevede l'azione a suffragio degli obiettivi aziendali, realizzata attraverso la consulenza destinata alle attività poste in essere.

Il "CoSO Report" avvalora questa visione declinando tale controllo come "*un insieme di azioni propositive condotte da un ente per promuovere adeguati comportamenti del proprio personale*".

Questo approccio innovativo ha prospettato un nuovo modo di esercitare attività bancaria, elevando tale sistema ad elemento necessario per il raggiungimento del successo aziendale.

Anche se non adeguatamente sottolineato nelle precedenti definizioni, rientra nella declinazione di controllo interno il concetto di sistema – ci si riferisce infatti al Sistema dei Controlli Interni – attraverso il quale indicare l'apparato di cui esso è costituito. Trattasi infatti di un complesso incardinato nell'organizzazione, che nasce contestualmente alla stessa.

Muovendo da tale considerazione il Sistema dei Controlli Interni è scomponibile in una pluralità di elementi: a esso fanno riferimento il personale, le risorse monetarie e quelle tecniche che nello svolgimento delle attività di controllo partecipano attivamente al raggiungimento degli obiettivi.

Le componenti a cui viene fatto riferimento non rappresentano però una mera sommatoria, ma il valore aggiunto che sono in grado di generare è frutto delle sinergie e del coordinamento che le uniscono. Si deve dunque scindere la struttura del sistema, che si compone degli elementi di cui i controlli interni si avvalgono compresi gli obiettivi formulati dai vertici aziendali, dal funzionamento dello stesso, frutto delle connessioni e dei rapporti sinergici che si sviluppano tra i soggetti deputati al controllo.

Al momento della definizione dell'organizzazione il management si preoccuperà di implementare la struttura del sistema, promuovendo l'integrazione ed il coordinamento tra i destinatari chiamati in causa e successivamente provvederà al mantenimento del complesso in relazione all'evoluzione dell'attività. Solo attraverso un'adeguata struttura è

auspicabile il corretto funzionamento, che necessita delle adeguate sinergie e competenze per un'attività di successo.

Struttura e corretto svolgimento sono i due elementi necessari per l'attuazione dell'azione di supporto descritta, entrambi aspetti caratterizzanti del sistema prescindendo dai quali viene a mancare l'adeguato sostegno alle attività. Mentre la componente organizzativa è illustrata nelle definizioni, quest'ultime non tengono in dovuta considerazione l'aspetto funzionale, assai più qualificativo dell'attività.

Spetta dunque all'Alta Direzione fornire la garanzia della realizzazione di un Sistema dei Controlli Interni idoneo a fornire il proprio contributo, curando al tempo stesso il profilo strutturale nonché quello funzionale, per mezzo di interventi organizzativi e di indirizzo.

1.2 Controlli interni, organizzazione aziendale e corporate governance

Come detto il Sistema dei Controlli Interni non rappresenta all'interno della struttura aziendale un processo attivabile saltuariamente per mezzo di verifiche di adeguatezza, ma si configura come un elemento costante e fortemente inglobato nell'organizzazione, dalla cui applicazione nel continuo l'azienda banca non può prescindere.

Il controllo interno non è la mera ispezione applicata all'esercizio dell'impresa bancaria ma risulta invece la componente della struttura portante organizzativa che l'intermediario adotta al momento della sua costituzione e mantiene, modifica ed aggiorna lungo l'arco della propria esistenza. Sistema dei Controlli Interni e organizzazione sono elementi strettamente connessi al punto tale da essere inscindibili ed inevitabili.

Il sistema, quale tassello della struttura aziendale è oggetto di particolare interesse da parte della Banca d'Italia, che ne valuta l'adeguatezza nello svolgimento della propria attività di vigilanza sugli intermediari.

L'attenzione è testimoniata dalla stessa Autorità di settore che sostiene "*come gran parte delle situazioni di difficoltà individuate nell'esercizio dell'attività di vigilanza sono collegabili ad assetti organizzativi inadeguati e a carenze nel sistema dei controlli interni*"[13].

Una tale attenzione riservata alla componente organizzativa è rivolta all'individuazione dei punti di debolezza all'interno di quest'ultima – e del sistema – per evitare che venga compromessa l'azione di presidio ai rischi che minacciano l'attività.

Da parte sua la Vigilanza si interessa del Sistema dei Controlli Interni attraverso una duplice azione che comprende, in primis la produzione di normativa secondaria che indichi gli standard di best practices per mezzo di principi e raccomandazioni rivolti alla gestione dei rischi aziendali, alla funzione di Revisione Interna, ai sistemi informativi ed alla gestione di una politica comune di gruppo. In secondo luogo svolge l'azione di verifica sui sistemi concretamente sviluppati dai singoli istituti secondo l'approccio basato sul rischio ed il principio di proporzionalità.

Con particolare riferimento a questi ultimi è opportuno fare un richiamo delle rispettive definizioni poiché spesso verranno ripresi nel prosieguo. Le origini dell'approccio basato sul rischio sono da ricercarsi negli standard del CoSO ed in particolare nel "Framework ERM" (Enterprise Risk Management) che contiene la seguente definizione di approccio basato sul rischio: *"la gestione del rischio aziendale è un processo, posto in essere dal consiglio di amministrazione, dal management e da altri operatori della struttura aziendale; utilizzato per la formulazione delle strategie in tutta*

[13] In BANCA D'ITALIA – "Bollettino di Vigilanza", numero 10 – Ottobre 1999.

l'organizzazione; progettato per individuare eventi potenziali che possono influire sull'attività aziendale, per gestire il rischio entro i limiti del rischio accettabile e per fornire una ragionevole sicurezza sul conseguimento degli obiettivi aziendali"[14].

Quanto invece al principio di proporzionalità, trae le proprie origini dalla normativa nazionale, e in particolare è inserito nel comma 2 dell'articolo 23 della Legge 28 dicembre 2005, n. 262 rubricata "Disposizioni per la tutela del risparmio e la disciplina dei mercati finanziari". Con esso si intende il "criterio di esercizio del potere adeguato al raggiungimento del fine, con il minore sacrificio degli interessi dei destinatari". Questa formulazione ha influenzato tutte le successive disposizioni normative in materia bancaria e finanziaria anche di secondo livello, ridefinendo il ruolo dell'Autorità di Vigilanza nei confronti dei singoli istituti. L'approccio ha spiegato i propri effetti attraverso la formulazione di obblighi meno prescrittivi in favore di più generali previsioni allo scopo di meglio adattarsi alle peculiarità del singolo istituto. In tal modo vengono valorizzate anche le capacità del management, che di fronte alla libertà di scelta dell'assetto organizzativo e di controllo deve adoperarsi per la realizzazione di un sistema coeso che permetta il raggiungimento degli obiettivi; la direzione assume un ruolo centrale nella predisposizione del Sistema dei Controlli Interni. Tuttavia il passaggio da un approccio rule-based ad uno risk-based (proporzionalità e approccio basato sul rischio sono elementi strettamente connessi tra loro, poiché adattare i controlli alle peculiarità dell'istituto significa soprattutto adattarli a grado di rischio che l'ente si trova a fronteggiare in ragione delle caratteristiche assunte), non deve essere erroneamente interpretato come libertà da vincoli ed arbitraria autogestione nell'esercizio del potere. Bensì – citando Dellarosa – "si tratta di un lassez-faire solo apparente, dato che l'auto-organizzazione deve informarsi al principio dell'idoneità dei

[14] Traduzione italiana curata da AIIA e PricewaterhouseCoopers.

provvedimenti rispetto alle finalità legislative e alla costante mitigazione dei rischi a carico della banca"[15].

Alla luce dell'introduzione dei principi citati, il rapporto tra istituti e vigilanza, a seguito anche dell'emanazione del nuovo accordo sul capitale, ha subito alcune modifiche: gli intermediari dovranno sì dotarsi di un'adeguata sicurezza patrimoniale in funzione del livello di rischio che si trovano a fronteggiare, ma ciò non può di per sé essere considerato sufficiente. Sotto la lente d'ingrandimento della Vigilanza sarà posta anche la struttura organizzativa ed il correlato sistema dei controlli, con la finalità di implementare all'interno del complesso aziendale adeguati presidi al rischio, nonché processi e procedure valutative degli stessi. Appare chiaro come anche l'atteggiamento di Banca d'Italia – oltre a quello della regolamentazione internazionale – consideri organizzazione e sistema dei controlli come elementi imprescindibili per la corretta gestione aziendale, i quali sommati a un'adeguata dotazione patrimoniale sono ragionevolmente in grado di portare al raggiungimento degli obiettivi. È dunque importante che il controllo costituisca il driver della cultura aziendale, allo scopo di realizzare la dovuta consapevolezza delle connesse problematiche organizzative e delle strutture e procedure di presidio. La creazione di un adeguato assetto organizzativo e di un Sistema dei Controlli Interni rientra tra le competenze del management con la finalità di raggiungere la correttezza gestionale e di mantenerla nel tempo. La stretta correlazione che lega controlli interni e organizzazione fino a confonderne i tratti, è già stata evidenziata; tuttavia vi è un'altra componente per nulla trascurabile che si inserisce nella relazione come elemento propulsivo: la corporate governance[16].

[15] In E. DELLAROSA – R. RAZZANTE, "Il nuovo sistema dei controlli interni della banca", Franco Angeli, Milano 2010.

[16] Definita dall'OECD come "procedures and processes according to which an organisation is directed and controlled. The corporate governance structure specifies the distribution of rights and

Prescindendo dalla forma assunta dal sistema di governo che fa capo a un intermediario, esso rappresenta l'elemento deputato alla formulazione degli obiettivi aziendali e all'organizzazione della struttura funzionale al raggiungimento degli stessi. La consapevolezza che il sistema dei controlli sia un utile strumento di governo deve nascere ai vertici dell'istituto che, di conseguenza, ne orientano la progettazione verso le esigenze palesate. È possibile affermare che il controllo rivolto alla buona gestione dei rischi aziendali è elemento qualificante di un buon sistema di governo societario, espressione della corretta gestione. Il management si trova infatti a orientare le sorti dell'impresa attraverso l'assunzione costante di decisioni, per le quali è assolutamente necessario disporre di un adeguato livello informativo in merito alle opportunità ed ai rischi che queste comportano, inoltre l'alta direzione deve anche essere in grado di gestire le minacce rilevate relativamente alle scelte compiute. L'attività di supporto così delineata è propria del sistema di controllo; appare dunque confermato il sostegno al raggiungimento della mission aziendale, fornendo una ragionevole sicurezza riguardo al successo delle scelte poste in essere. In definitiva il buon governo di un istituto passa attraverso le tre componenti enunciate di corporate governance, struttura organizzativa e Sistema dei Controlli Interni e solo attraverso il giusto coordinamento e la presa di coscienza del valore di questi ultimi è possibile ottenere la ragionevole sicurezza riguardo al raggiungimento degli obiettivi comuni.

1.3 La struttura del Sistema dei Controlli Interni

L'approccio sin qui adottato nella considerazione del sistema dei controlli ha visto la distinzione tra elementi strutturali – cioè la componente

responsibilities among the different participants in the organisation – such as the board, managers, shareholders and other stakeholders – and lays down the rules and procedures for decision-making".

organizzativa che incardina il sistema all'interno della struttura aziendale – ed elementi funzionali, quelli concretamente utilizzati nell'esercizio dell'attività di supporto. Quanto ai primi verrà data spiegazione di seguito, con una precisazione in merito ai soggetti destinatari di funzioni di controllo interno, mentre nel paragrafo successivo verrà fornita indicazione delle metodologie proprie del controllo. L'elemento basilare della struttura del sistema sul quale poggiano le altre componenti è la cultura aziendale, o più nello specifico la cultura del controllo. Ogni istituto genera al proprio interno la cultura aziendale, cioè l'insieme di filosofia e valori ai quali l'intera organizzazione si deve ispirare nell'esercizio delle proprie funzioni. È il valore che gli organi gestionali devono essere in grado di creare e trasmettere, affinché esso venga riflesso negli atteggiamenti del personale con convinzione. Per gli istituti bancari è importante che la cultura aziendale sia principalmente una "*cultura del controllo*".

Il Consiglio di Amministrazione e la Direzione devono prodigarsi affinché tra i valori fondamentali ai quali il personale si ispira vi rientri l'idea che il controllo è un elemento determinante nel successo delle politiche aziendali.

Ciò presuppone che sia l'Organo di Supervisione Strategica (C.d.A.) in primis ad apprezzare il contributo che il Sistema dei Controlli Interni è in grado di fornire nella preservazione dell'attività dai rischi ed il sostegno nel raggiungimento dei comuni obiettivi fissati. È di competenza del management la creazione e la diffusione della cultura aziendale all'interno dell'organizzazione e solo attraverso l'apprezzamento totale da parte di quest'ultimo potranno essere divulgati correttamente i valori di controllo ed avversione al rischio.

Per una realizzazione di successo è importante che il messaggio penetri nelle menti del personale e venga metabolizzato come una visione imprescindibile dell'attività bancaria, solo in questo modo l'approccio

orientato al rischio potrà lasciare la propria impronta nelle singole attività compiute. La divulgazione di questo modus operandi non è certo immediata né indolore poiché arreca con sé il cambiamento, nei confronti del quale il personale è spesso reticente.

Inoltre frequentemente non si comprende appieno che la cultura aziendale è unica e come tale universalmente accettata ad ogni livello; non è perciò ammissibile la visione che confini la cultura del controllo limitatamente ai soggetti destinatari di tali funzioni all'interno del sistema. Sarà la cultura nella sua interezza a mutare, sensibilizzando riguardo alle tematiche del rischio e rivolgendosi alla totalità del personale inserito nelle diverse strutture.

Agli organi con funzioni di gestione (tradizionalmente Consiglio di Amministrazione e Direzione) è dunque affidata la responsabilità della creazione e della divulgazione della cultura aziendale rivolta alla valorizzazione dei controlli interni, verificando che venga concretamente recepita e costantemente richiamata nello svolgimento di ogni attività intrapresa dal personale.

Per essere credibile la cultura del controllo deve essere formalizzata acquistando così stabilità e coerenza, ma non per questo deve essere esente da revisioni in funzione dell'evoluzione degli standard di riferimento.

Appurata la necessità di una cultura del controllo fortemente radicata e concretamente attuata dall'intera organizzazione, il secondo elemento attinente alla struttura del Sistema dei Controlli Interni riguarda proprio l'organizzazione di quest'ultimo e la suddivisione delle relative attività di controllo fra le diverse unità aziendali interessate. Muovendo dalla considerazione che non esiste un modello unico di sistema che possa definirsi migliore in assoluto, in ragione del principio di proporzionalità e dell'approccio basato sul rischio, saranno possibili svariate soluzioni tutte

allo stesso modo valide. Tuttavia i canoni interpretativi utilizzati dall'alta direzione nella predisposizione di un corretto assetto organizzativo – quale esso sia – hanno in comune alcuni elementi guida che possono contribuire alla realizzazione di una struttura di successo.

Come ampiamente suggerito dalla regolamentazione secondaria anche di natura internazionale, è importante che la predisposizione di un sistema di controllo si accompagni a una chiara formalizzazione dei contenuti rivolti all'individuazione di compiti e responsabilità in capo ai soggetti coinvolti in attività di controllo. Il management deve, sempre coerentemente con le politiche adottate e le finalità preposte, istituire e mantenere nel tempo un'adeguata architettura organizzativa avendo cura di individuare i soggetti destinatari di competenze e responsabilità. A esso spetta anche la definizione delle relazioni gerarchiche che mettono in connessione i soggetti interessati. Attraverso la formalizzazione dei ruoli viene reso noto all'interno dell'organizzazione quali siano i soggetti interessati da attività di controllo interno ed allo stesso modo quale sia l'ampiezza dei poteri loro riservati che determina il grado di responsabilità assunte. I vertici nella scelta della struttura ottimale possono ricercare liberamente il miglior modello al quale ispirarsi, ma è imprescindibile che la soluzione adottata venga pubblicizzata nel complesso aziendale attraverso una comunicazione che non lasci spazio ad interpretazioni equivoche.

Per la realizzazione di un efficiente sistema di controllo il personale deve conoscere il ruolo che è chiamato a svolgere, allo stesso modo deve essere conscio delle relazioni intrattenute con altre unità organizzative e infine avere cognizione delle linee di riporto.

Sul tema le Autorità di Vigilanza dispongono che gli istituti applichino e mantengano "*idonei meccanismi di controllo interno volti a garantire il rispetto delle decisioni e delle procedure a tutti i livelli*" e inoltre che "*il*

personale sia provvisto delle qualifiche, delle conoscenze e delle competenze necessarie per l'esercizio delle responsabilità attribuite"[17].

L'Organo di Supervisione Strategica ha infine il compito di monitorare costantemente il funzionamento dell'assetto organizzativo prescelto, garantendo che l'attività sia svolta da personale competente e dotato delle risorse necessarie per ammontare e caratteristiche. Un ulteriore elemento di assoluta rilevanza che delinea la struttura del sistema di controllo aziendale è costituito dalle politiche di rischio. Come già esposto, l'attività bancaria è stata innovata attraverso il framework del Comitato di Basilea che ha promosso la gestione orientata al rischio attraverso il risk based approach. È dunque necessario che l'impresa bancaria, al fine di realizzare un'adeguata struttura di presidio, stabilisca il proprio "profilo" di rischio sulla base degli obiettivi fissati. L'Alta Direzione deve dunque formulare la politica di rischio in diretta conseguenza dell'orientamento strategico assunto nell'attuazione del governo, con la finalità di raggiungere la necessaria coerenza tra risultati ed insidie.

La definizione della linea di condotta passa attraverso l'individuazione preliminare delle minacce in grado di interessare il business aziendale e solo successivamente ad un'analisi attenta e mirata è possibile predisporre adeguati presidi, potendo ricondurre il grado di rischio a livelli ritenuti accettabili. Si tratta di ricercare il giusto equilibrio tra obiettivi di performance, che si concretizzano in crescita e profittabilità e la conservazione dell'attività bancaria dalle minacce ad essa connesse. Il management è chiamato a operare una scelta complessa di trade-off, assumendo il livello di rischio che è disposto a tollerare e definendo il complesso dei presidi da realizzare per mantenere il livello di minaccia entro la soglia preventivamente stabilita. Ciò determina appunto la politica

[17] Da "Regolamento della Banca d'Italia e della CONSOB ai sensi dell'articolo 6, comma 2-bis, del Testo Unico della Finanza", comma 2, art. 5, lettere d) ed e).

di rischio propria dell'impresa, ossia la tolleranza con la quale l'Alta Direzione si rapporta, nonché l'insieme delle misure di prevenzione. Attraverso la stessa si realizza altresì l'articolazione ed il concreto funzionamento del complesso Sistema dei Controlli Interni. Tale programma di gestione rappresenta inoltre l'espressione della consapevolezza del Consiglio di Amministrazione in materia di rischi, rispetto ai quali dovrà rivolgere costantemente la propria attenzione, pronto a cogliere situazioni di cambiamento che originano dalla dinamica del business aziendale.

Infine è opportuno precisare come le politiche si adattino – oltre all'attività svolta – alla tipologia di minacce affrontate: qualora i rischi siano valutabili e quantificabili si fa loro riferimento in termini quantitativi, se invece per gli stessi non fosse possibile operare una misurazione l'approccio più idoneo risulterebbe quello qualitativo.

1.4 L'aspetto funzionale del Sistema dei Controlli Interni

Analizzati gli aspetti organizzativi essenziali del Sistema dei Controlli Interni, l'attenzione viene ora focalizzata sulla componente funzionale del controllo interno allo scopo di indagare quali elementi contribuiscano all'attuazione dell'attività di controllo; da un'indagine sulla componente statica – la struttura – si passa all'aspetto dinamico del sistema: il suo funzionamento.

Ancora una volta è necessario sottolineare come anche per l'elemento operativo non esistano modelli di riferimento considerabili concreta espressione della best practice regolamentare di derivazione internazionale. Come per l'aspetto strutturale, allo stesso modo il principio di proporzionalità e l'approccio basato sul rischio costituiscono capisaldi ai

quali il management deve fare riferimento nella fase di progettazione e di manutenzione (rinnovamento) del sistema. Il concreto esercizio dell'attività di controllo sarà perciò svolto in maniera difforme da istituto a istituto, secondo gli obiettivi aziendali stabiliti, in ragione della complessità strutturale ed operativa, nonché valutando il livello di rischiosità secondo la politica di rischio assunta. La principale delle attività – la vocazione naturale per la quale ha origine il sistema dei controlli – è la preservazione dell'azienda dalle minacce che possono distoglierla dal raggiungimento degli obiettivi stabiliti dall'organo gestorio. La dottrina in materia[18], traendo spunto dalle disposizioni di vigilanza prudenziale, individua tale attività nella valutazione complessiva dei rischi aziendali. In particolare in Pesic è possibile leggere: "nella componente di valutazione del rischio, che all'interno dell'intermediario creditizio è individuata con il concetto più ampio di gestione del rischio, si tiene conto dell'attività di individuazione, valutazione e gestione dei diversi fattori di rischio interni ed esterni, in grado di influire negativamente sul conseguimento degli obiettivi aziendali". L'attività di risk management[19] così delineata riflette dunque le sembianze dell'operatività bancaria indirizzata dall'alta direzione.

Secondo tale impostazione si è giunti ad un approccio di gestione accentrata delle minacce, attraverso una valutazione generale in grado di quantificare in modo complessivo l'esposizione dell'attività bancaria.

Strumentale a tale impostazione è la predisposizione, ad opera del management, di adeguate soluzioni che permettano l'identificazione, la misurazione ed il controllo dell'esposizione sia in relazione ai singoli fattori di rischio, nonché alle minacce originate da influenze reciproche. Tale

[18] Il riferimento è a Pesic ne "Il Sistema dei Controlli Interni nella banca" e sulla medesima linea Dellarosa ne "Il nuovo sistema dei controlli interni della banca".
[19] Saita ne "Il risk management in banca" definisce la gestione del rischio come il complesso delle metodologie e dei processi volti alla misurazione e al controllo integrato dei rischi della banca, finalizzati alla efficiente gestione in chiave dinamica del capitale proprio a disposizione.

approccio permette la reconductio ad unum della valutazione del rischio globale.

Nell'organizzazione dell'attività di gestione del rischio l'alta direzione deve assicurarsi che l'unità destinataria dei compiti sia caratterizzata da indipendenza in grado di portare ad una valutazione obiettiva e affidabile della situazione aziendale, orientata al controllo delle aree dove il rischio ha origine, che riporti direttamente all'organo direttivo e che sia sottoposta a verifica da parte della revisione interna.

L'attività di risk management trova applicazione concreta attraverso il processo ad essa asservito, che attraverso il susseguirsi di determinate fasi operative realizza la complessa attività di gestione coinvolgendo l'intero ambiente aziendale. Tale processo giunge a compimento attraverso:

- un fase preliminare di mappatura dei rischi e delle attività in grado di generarli allo scopo di realizzare il quadro complessivo delle minacce aziendali;
- la valutazione di impatto dei riscontri ottenuta attraverso la misurazione della dimensione quantitativa e l'espressione di un giudizio sull'aspetto qualitativo;
- l'assunzione dei rischi;
- l'azione di contrasto alle minacce attraverso la predisposizione di presidi per la mitigazione, o più in generale per mezzo di azioni in risposta ai fenomeni;
- la fase terminale di monitoraggio costante dell'evoluzione dei rischi riscontrati, di quelli inediti scaturiti dall'evoluzione del business e del corretto funzionamento delle soluzioni adottate.

Il processo di gestione, attraverso le fasi successive di cui si compone, non solo coinvolge interamente il sistema dei controlli dal quale trae origine e viene alimentato, ma interessa anche componenti dell'organizzazione che

non si occupano specificamente di controllo. Ne è esempio la fase di assunzione dei rischi, che essendo strettamente connessa al raggiungimento dei risultati prefissati non può che essere assunta nella responsabilità degli organi direttivi.

Il processo è dunque un'attività che attraversa l'intera organizzazione aziendale ed alla quale sono chiamati a partecipare – secondo modalità differenti – tutte le unità che la compongono.

In ragione di un simile approccio appare ancor più giustificabile la corretta diffusione di una cultura aziendale guidata dal controllo, quale elemento strutturale portante di un'adeguata gestione del rischio.

L'alta direzione ha dunque la responsabilità di progettare l'apparato di gestione del rischio – risk management – sulla base del miglior modello applicabile all'impresa allo scopo di determinare, quantificare e mitigare le manifestazioni che possano ostacolare il raggiungimento degli obiettivi ed inoltre assicurare nel tempo che le soluzioni adottate siano sempre adeguate, in funzione dell'evoluzione dell'attività.

Un apporto rilevante all'attività di gestione del rischio e più in generale all'intero Sistema dei Controlli Interni è fornito dai flussi informativi volti ad assicurare l'azione informata dei soggetti che vi partecipano. Attraverso la conoscenza e la comunicazione si rende possibile la diffusione all'interno dell'ambiente dei dati e delle notizie necessari all'attività di controllo, il personale viene edotto in merito alla politica di rischio ritenuta ottimale ed il management ottiene i feedback necessari alla supervisione del sistema, nonché all'assunzione di decisioni informate.

A tale aspetto i framework internazionali hanno assegnato forte rilevanza, come testimoniato dal Comitato di Basilea il quale sottolinea la necessità per il controllo interno di essere supportato adeguatamente da sistemi informativi e canali di comunicazione. Si legge che "un efficace sistema di

controllo interno richiede che operino affidabili sistemi informativi comprendenti tutte le attività rilevanti della banca. Tali sistemi, inclusi quelli che contengono e utilizzano dati in forma elettronica, devono essere sicuri, sorvegliati in modo indipendente e assistiti da adeguati dispositivi di emergenza"[20].

Gli istituti devono dunque dotarsi di un sistema basato su tecnologie elettroniche, in grado di raccogliere il patrimonio informativo in materia di attività di controllo e gestione del rischio. È altresì importante che vengano garantiti un adeguato livello di significatività dei dati, l'affidabilità degli stessi in merito al contenuto, la tempestività della disponibilità ed accessibilità da parte dei soggetti titolati al loro utilizzo.

Altra caratteristica che interessa le informazioni è l'uniformità che deve riguardare il loro trattamento, potendo in questo modo assicurare un'interpretazione univoca del suo contenuto ed una gestione integrata. Allo stesso modo assume rilevanza la circolazione di tali informazioni, che deve essere strutturata in appositi canali a seconda della tipologia dei dati diffusi. Questi infatti si sviluppano secondo una direttrice verticale quando hanno finalità di reporting, permettendo al management ed alla direzione di prendere coscienza della reale situazione che interessa il sistema dei controlli – con particolare riguardo all'efficacia dei presidi adottati, alla valutazione dei rischi affrontati ed al riscontro di carenze –, ma anche allo scopo di diffondere la politica di rischio e le indicazioni sull'approccio da adottare nella gestione.

Diversamente la diffusione delle informazioni si sviluppa anche all'interno dell'organizzazione per vie orizzontali, coinvolgendo le differenti unità interessate nell'attività di controllo, ma più in generale i flussi toccano in

[20] BASEL COMMITTEE ON BANKING SUPERVISION, "Schema per i sistemi di controllo interno nelle organizzazioni bancarie", 1998, principio n. 8.

vario modo tutto il personale dato il forte legame tra Sistema dei Controlli Interni ed organizzazione aziendale nel suo complesso.

L'alta direzione nello svolgimento della propria attività di gestione deve necessariamente predisporre un sistema aziendale che permetta la certezza della comunicazione e della diffusione delle informazioni in materia di controllo, al fine di creare consapevolezza nel personale e sensibilizzazione ai temi, ma soprattutto permettendo l'agire informato che riguarda in primo luogo il management stesso.

In relazione a quanto finora affrontato, l'istituto ha come ultima necessità quella di assicurare che il Sistema dei Controlli Interni e la connessa attività di gestione del rischio, mantengano i livelli di adeguatezza ed efficienza raggiunti lungo il periodo nel quale il business si svolge. L'organo gestorio deve compiere azioni di monitoraggio e verifiche periodiche – anche avvalendosi di altri soggetti interni ed esterni – volte ad individuare disallineamenti tra la politica di rischio stabilita e la concreta realizzazione delle attività di controllo, nonché valutare le nuove situazioni in grado di arrecare danno all'attività. Il monitoraggio prevede un'azione di supervisione continua a carattere generale sui controlli interni, le verifiche saranno invece mirate all'indagine di particolari aspetti o processi, per le quali il management potrà avvalersi del supporto della funzione di Revisione Interna.

1.5 Le componenti del Sistema di Controllo Interno

Secondo la già citata definizione fornita dal *Committee of Sponsoring Organizations of the Treadway Commission*, nella fondamentale opera *Internal Control - Integrated Framework, AICPA, New York, 1992 (COSO Report)*, si ribadisce che per sistema di controllo interno si intende un

processo, svolto dal Consiglio di Ammnistrazione, dai Dirigenti e da altri soggetti della struttura aziendale, finalizzato a fornire una ragionevole sicurezza sul conseguimento degli obiettivi riconducibili all'efficacia ed efficienza delle attività operative, all'attendibilità delle informazioni di bilancio e alla conformità alle leggi e ai regolamenti in vigore.

Dopo averne delineato le sue caratteristiche di governance, è coerente analizzarne la struttura in termini di componenti.

Il sistema di controllo interno è composto da cinque elementi, tra loro interrelati:

- Ambiente di Controllo.
- Valutazione dei Rischi.
- Attività di Controllo.
- Informazione e comunicazione.
- Monitoraggio.

L'*Ambiente di controllo* si configura come l'elemento di cultura aziendale che determina il livello di sensibilità del personale alle esigenze di controllo. Esso costituisce la base per tutte le altre componenti del sistema di controllo interno. I fattori che influenzano l'ambiente di controllo sono l'integrità, i valori etici e la competenza del personale; la filosofia e lo stile gestionale del management; le modalità di delega delle responsabilità, di organizzazione e di sviluppo professionale e l'impegno e la capacità di indirizzo e di guida del Consiglio di Amministrazione.

Valutazione dei rischi. Ogni azienda deve essere consapevole dei rischi che incontra e che deve affrontare. Essa deve porsi obiettivi per le attività commerciali, finanziarie, di produzione, di marketing e altre, reciprocamente integrati affinché l'organizzazione possa operare in modo coordinato e armonico. Essa deve anche attivare i meccanismi che consentono di individuare, analizzare e gestire i rischi relativi.

Per *attività di controllo* s'intendono le politiche e le procedure di controllo che assicurano al management che le sue direttive siano applicate. Esse agevolano l'adozione di provvedimenti necessari per far fronte ai rischi che potrebbero pregiudicare la realizzazione degli obiettivi aziendali. Le attività di controllo si attuano in tutta l'organizzazione ed in tutti i suoi livelli. Esse comprendono un insieme di attività diverse come approvazioni, autorizzazioni, verifiche, raffronti, esami della performance operativa, protezione dei beni aziendali e separazione dei compiti.

Informazione e comunicazione: attorno alle suddette attività di controllo si collocano i sistemi di informazione e comunicazione. Questi consentono al personale la raccolta e lo scambio delle informazioni necessarie alla gestione e al controllo. Le informazioni pertinenti devono essere individuate, rilevate e diffuse nei modi e nei tempi appropriati per consentire alle persone di assolvere le proprie responsabilità. Comunicazioni efficaci devono inoltre sussistere verso il basso, verso l'alto e trasversalmente alla struttura organizzativa. Il management deve trasmettere un messaggio chiaro a tutto il personale sull'importanza delle responsabilità in materia di controllo. Il personale deve rendersi conto del proprio ruolo nell'ambito del Sistema di Controllo Interno, nonché di come le singole attività siano correlate al lavoro degli altri. Il personale deve disporre di mezzi per comunicare le informazioni di rilievo verso la parte alta della scala gerarchica. Inoltre, sono necessarie comunicazioni efficaci con i terzi, come clienti, fornitori, autorità tutorie e azionisti.

Monitoraggio. L'intero processo di controllo deve essere monitorato mediante un processo diretto a valutare la qualità delle performance nel tempo. Ciò si concretizza in attività di supervisione continua, in valutazioni periodiche oppure in una combinazione dei due metodi. La supervisione si esplica nell'ambito della gestione corrente e comprende normali attività di controllo effettuate da dirigenti e funzionari, nonché altre iniziative assunte

dal personale nello svolgimento delle proprie mansioni. La portata e la frequenza delle valutazioni periodiche dipenderà principalmente dalla valutazione dei rischi e dall'efficacia delle procedure di supervisione. Le carenze di controllo interno dovranno essere sempre segnalate verso l'alto e, nei casi più gravi, fino ai massimi vertici aziendali e al Consiglio di Amministrazione.

Si consideri che le cinque componenti del sistema di controllo interno non devono essere considerate come separate, ma anzi sono inevitabilmente interconnesse.

Come già detto nei paragrafi precedenti, il sistema di controllo interno è un processo e non un evento isolato: "é un mezzo mirato a un fine, non un fine di per se stesso".

1.6 Le funzioni di controllo interno

L'organizzazione assume il ruolo di elemento principale nella realizzazione del Sistema dei Controlli Interni in concordanza con le altre componenti strutturali, quali l'ambiente interno e le politiche di rischio. Nel considerare l'aspetto strutturale risulta rilevante indagare come le attività di controllo vengano distribuite tra le diverse unità organizzative che compongono tale sistema, contribuendo in questo modo alla realizzazione del modello adottato in relazione alla politica di rischio.

È utile precisare come anche questo aspetto venga interessato dal già noto principio di proporzionalità, più volte richiamato contestualmente al risk based approach, non contemplando quindi per gli istituti un modello preferenziale che sia espressione della migliore soluzione. Tuttavia le disposizioni di vigilanza di Banca d'Italia prevedono esplicitamente

l'indicazione di organi e unità organizzative che gli istituti non possono trascurare di costituire presso la propria struttura e rispetto ai quali vengono fornite indicazioni sulle attività da svolgere nel contesto dei controlli interni. L'Autorità di Vigilanza fornisce indicazioni attraverso la statuizione di principi di best practices rispetto ai quali ogni singolo istituto deve trarre ispirazione nella realizzazione e nella manutenzione nel tempo di un adeguato impianto di controllo rispondente alle specifiche peculiarità. Con particolare riferimento alla normativa secondaria di vigilanza diffusa da Banca d'Italia, in essa viene fatto riferimento alle funzioni di controllo delle quali gli istituti devono dotarsi nell'attuazione del presidio dei rischi e definite dalla dottrina come "*l'insieme delle attività volte a favorire il raggiungimento degli obiettivi aziendali secondo i principi e le regole del sistema dei controlli interni"*[21].

È però necessario precisare sin da subito come il concetto di funzione attenga alle attività che vengono assegnate alle diverse unità organizzative investite dell'attività di controllo. In particolare il riferimento è al complesso "*di poteri, competenze, compiti ed attività previste dal sistema dei controlli interni per il raggiungimento di determinate finalità di presidio, calate nella struttura organizzativa aziendale*"[22].

Dette funzioni vengono poi destinate, sulla base delle indicazioni delle disposizioni normative e regolamentari, ai diversi soggetti coinvolti nel sistema.

Tuttavia, la terminologia corrente ha avvicinato molto i concetti di funzione e di unità organizzativa (ovvero organo), sino a portare alla confusione dei concetti, intendendo con funzione anche l'unità organizzativa destinataria dei compiti e delle responsabilità.

[21] Dellarosa ne "Il nuovo sistema dei controlli interni nella banca".
[22] In Dellarosa ne "Il nuovo sistema dei controlli interni nella banca".

Ciò è spiegabile attraverso l'elevata specificità delle attività assegnate che necessitano la gestione da parte di un'unità a esse dedicata: ne è un esempio in tal senso la funzione – appunto – di compliance per mezzo della quale si realizza la conformità alle norme che interessano l'intermediario e con la quale viene altresì intesa l'unità Compliance ad essa asservita.

Differenti considerazioni possono invece riguardare la funzione antiriciclaggio – per la quale non esiste al momento una univoca destinazione, ma la soluzione organizzativa viene lasciata alla discrezionalità del singolo istituto – stante ad indicare la sola attività di presidio dal rischio di riciclaggio.

Ciò premesso è rilevante indagare come tali funzioni di controllo vengano distribuite all'interno dell'organizzazione e in particolare entro il perimetro del sistema di controllo, ma altresì come possano interessare, con modalità difformi, l'intera organizzazione ed il coinvolgimento di tutto il personale. Facendo costante riferimento all'assetto organizzativo, strettamente interlacciato con il concetto di controlli interni, è possibile operare una ripartizione delle funzioni tra organi, funzioni aziendali di controllo tipiche e funzioni aziendali di controllo in senso lato.

Attraverso la prima categoria – gli organi – la normativa secondaria di vigilanza emessa da Banca d'Italia individua con essa, riferendosi al sistema di corporate governance tradizionale, il Consiglio di Amministrazione, il Collegio Sindacale ed il Direttore Generale. Tali soggetti sono coinvolti necessariamente in attività di controllo sulla base delle normative che li interessano, ma anche per la naturale vocazione al raggiungimento degli obiettivi prefissati. Il coinvolgimento degli organi è riassumibile come di seguito.

- Il Consiglio di Amministrazione – e più in generale l'organo destinatario di funzioni di supervisione strategica – è coinvolto nei

controlli interni attraverso la formulazione della politica di rischio e nella realizzazione della struttura del Sistema dei Controlli Interni, tenendo in considerazione le peculiarità dell'intermediario e le tipologie di rischio affrontate. Inoltre realizza le strategie e le direttive alle quali il personale si deve attenere e si assicura che compiti e responsabilità siano correttamente allocati. Altresì deve promuovere all'interno dell'organizzazione i valori e la cultura del controllo e verificare nel tempo che le azioni intraprese vengano effettivamente poste in atto ed infine il mantenimento in efficienza del sistema.

- Il Collegio Sindacale – e tutti gli organi con funzioni di controllo – svolgono un'azione di supervisione e coordinamento del Sistema dei Controlli Interni, assicurando che l'attività di tali controlli venga svolta secondo efficacia ed efficienza. Inoltre sovraintende e coordina le unità organizzative assegnatarie delle funzioni di controllo.
- La Direzione Generale – quale organo con funzioni di gestione – è chiamata alla verifica dell'applicazione nel concreto delle politiche predisposte dall'amministrazione ed in particolare cura il generale funzionamento delle attività di controllo e l'adeguatezza della struttura organizzativa predisposta, rispetto alle necessità dell'attività bancaria.

Per quanto riguarda invece le funzioni aziendali di controllo, esse costituiscono le attività che in maniera più diretta si occupano del presidio dei rischi, ma allo stesso tempo – secondo la terminologia corrente utilizzata – i soggetti assegnatari delle stesse.

Tali funzioni rispondono alle direttive predisposte dai vertici aziendali e contribuiscono alla realizzazione del quadro generale del sistema dei controlli attraverso l'attività strumentale di traduzione nel concreto della

politica di rischio. Tali funzioni vengono suddivise in tipiche, quelle cioè la cui presenza all'interno dell'organizzazione è prevista dalle normative e dai regolamenti in materia e sono proprie della struttura organizzativa degli intermediari. Ad esse si affiancano le funzioni in senso lato, previste da disposizioni settoriali e non endemiche dell'attività finanziaria. Le funzioni aziendali di controllo tipiche sono così riassumibili.

- La funzione di Revisione Interna risponde direttamente al Consiglio di Amministrazione e si caratterizza per lo svolgimento di verifiche volte a riscontrare l'efficacia e l'efficienza di aree, processi e procedure realizzati in azienda, ponendo sotto particolare attenzione l'allineamento tra le disposizioni impartite dalla direzione e l'attuazione delle stesse nel concreto. Tale azione di controllo si caratterizza per l'approccio ex-post, improntato cioè a verifiche successive delle soluzioni adottate nell'attività di controllo.
- La funzione Compliance partecipa al sistema attraverso un'azione continua di controllo volta ad asseverare la conformità a norme e regolamenti – di qualsiasi fonte – ai quali gli istituti sono soggetti nell'esercizio delle attività finanziaria e di credito.

L'attività ha origine attraverso l'identificazione delle norme già esistenti, di nuova emanazione, nonché delle modifiche alle stesse, le quali comportano nuove soluzioni ed adeguamenti allo scopo di allineare l'operatività bancaria a tali previsioni. L'approccio è sia di tipo ex-ante, realizzato per mezzo di valutazioni preventive delle esposizioni, sia ex-post quale riscontro dell'adeguatezza delle soluzioni adottate. Inoltre la funzione partecipa all'attività di valutazione dell'impatto di tali disposizioni sul complesso aziendale e formula proposte organizzative adeguate all'evoluzione degli obblighi e dell'attività bancaria.

- La funzione di controllo sulla gestione del rischio si assicura che l'attività di risk management sia attuata per mezzo delle fasi predisposte e secondo il corretto svolgimento delle stesse ed inoltre svolge azione di sorveglianza sull'esposizione dell'attività bancaria ai rischi.
- Le funzioni di controllo di linea svolgono azione di presidio direttamente all'interno delle unità operative nelle quali sono inserite, allo scopo di realizzare la concreta azione di mitigazione ed eliminazione delle minacce, in attuazione delle strategie e delle direttive predisposte dai vertici aziendali. È questa la fase attraverso la quale la politica di rischio e le azioni intraprese a realizzazione della stessa trovano riscontro in merito all'adeguatezza, nonché sulla quale basarsi per attuare azioni correttive di miglioramento.
- Le funzioni di Revisione Interna, Compliance e Risk Management operano secondo le disposizioni contenute dalla direttiva europea 2004/39/CE in materia di mercati e strumenti finanziari, meglio conosciuta come MiFID – Markets in Financial Instruments Directive.

Alcuni esempi di funzioni aziendali di controllo in senso lato sono invece sintetizzabili come segue.

- La funzione di prevenzione dei reati che comportano il coinvolgimento per responsabilità amministrativa dell'ente, affidata all'Organismo di Vigilanza come disposto dal d.lgs. 231/2001.
- La funzione di antiriciclaggio rivolta all'osservanza delle normative in materia di contrasto del riciclaggio e del finanziamento del terrorismo, allo scopo di prevenire la complicità inconsapevole degli istituti in tale attività illecita.
- La funzione volta a garantire il rispetto del trattamento dei dati personali raccolti dall'intermediario nell'instaurazione dei rapporti

con la clientela ed in qualsiasi altro modo acquisite, comprese le informazioni raccolte in osservanza delle disposizioni in materia di antiriciclaggio e finanziamento del terrorismo.

- La funzione destinata al rispetto delle disposizioni in materia di sicurezza sul posto di lavoro.

La normativa di vigilanza di Banca d'Italia prevede per le funzioni aziendali di controllo tipiche un'ulteriore ripartizione.

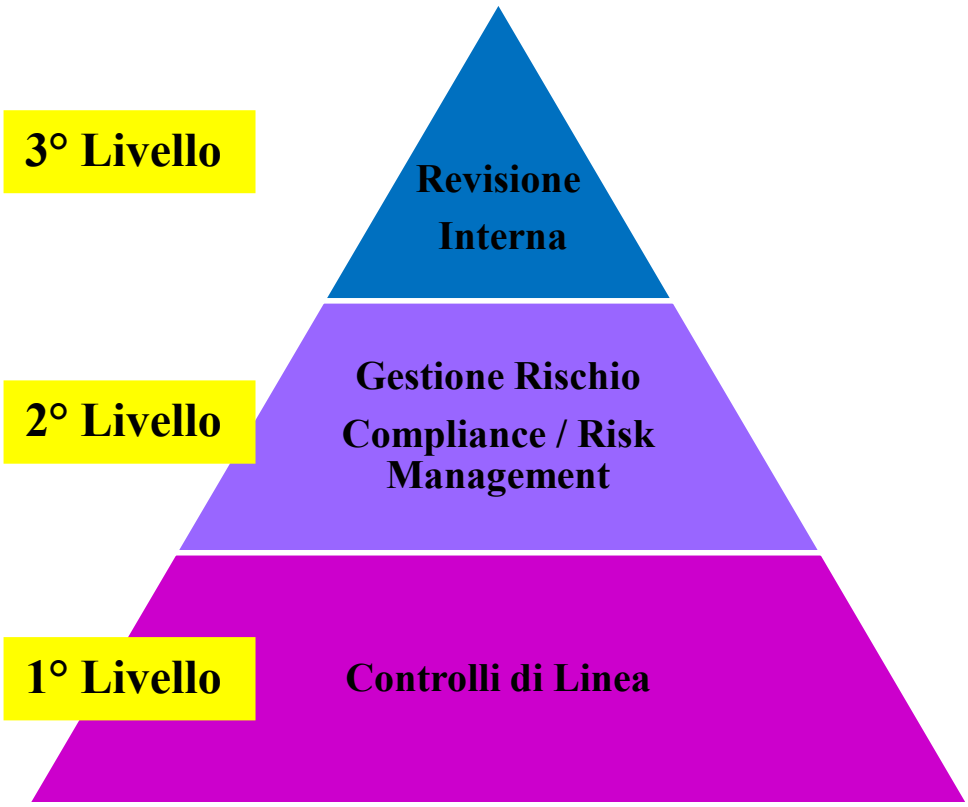
Le unità organizzative destinatarie, nello svolgimento delle funzioni che direttamente le riguardano, portano a compimento una serie di compiti che si differenziano in ragione della finalità che gli stessi mirano a perseguire, in funzione della tipologia di rischio presidiato, nonché delle caratteristiche proprie dell'unità assegnataria.

Le funzioni in oggetto vengono comprese nel più ampio processo di gestione del rischio e si avvalgono del Sistema dei Controlli Interni, nonché dell'intera organizzazione aziendale, allo scopo di supportare e garantire ragionevolmente il raggiungimento degli obiettivi; a ciascuna di esse è affidato lo svolgimento di compiti omogenei rispetto ai quali è possibili attuare un'ulteriore suddivisione in categorie, di seguito illustrate.

- Controlli di primo livello che riguardano i presidi di linea svolti all'interno delle unità operative. Essi rappresentano la prima linea di controllo e sono incaricati della concreta attuazione dei compiti secondo le metodologie predisposte dai gestori del rischio.
- Controlli di secondo livello sono svolti dalle funzioni Compliance e Risk Management e mirano alla gestione dei rischi attraverso l'implementazione di diverse soluzioni orientate alla valutazione dell'esposizione alle minacce, alla verifica dell'attività di controllo assegnate alle unità produttive ed al riscontro della coerenza tra

politica di rischio ed obiettivi di performance assegnati alle strutture operative.

- Controlli di terzo livello assegnati alla revisione interna, con la finalità di verificare l'adeguatezza riguardante il complesso delle Interni.



1.7 La classificazione dei rischi nelle disposizioni di vigilanza di Banca d'Italia

Gli istituti di credito in ragione delle tipologie di attività svolte sono da sempre stati interessati da un elevato livello di rischiosità, che tuttavia negli ultimi anni è accresciuto, alla luce dell'aumento della competitività del mercato nonché del novero dei servizi prestati al pubblico.

A fianco della tipica attività bancaria di concessione del credito e di prestazione di servizi legati alla raccolta rivolta a privati ed imprese, è possibile constatare la convivenza di un'ampia offerta di soluzioni di investimento attraverso tipologie differenti di strumenti finanziari ed in alcuni casi anche la prestazioni di servizi assicurativi.

La forte espansione dell'attività è stata accompagnata inesorabilmente all'ampliamento dei fattori di rischio che possono ostacolare il raggiungimento degli obiettivi aziendali. Secondo l'accezione più ampia il rischio comprende tutti i fatti di gestione la cui manifestazione è afflitta da incertezza e – qualora si verificassero – l'esito potrebbe essere favorevole o avverso al raggiungimento degli obiettivi aziendali. Il rischio che si manifesta in tali termini è definibile come "dinamico", poiché in grado di dare origine a conseguenze sia positive che negative.

Quando invece la manifestazione del rischio può arrecare esclusivamente conseguenze avverse all'impresa, si fa riferimento ad esso come ad un rischio "statico". Ne è un esempio in tal senso la minaccia rappresentata da frodi interne all'organizzazione, poste in essere dal personale dipendente di dubbia professionalità e basso livello morale. Quanto al rischio dinamico ne è un esempio quello di tasso di interesse, rispetto al quale la variazione che si origina può comportare una perdita di risorse per l'intermediario, piuttosto che un incremento delle stesse. Tuttavia in merito a questa seconda tipologia gli istituti rivolgono la loro attenzione all'aspetto negativo degli stessi, in grado di deviare la gestione dal raggiungimento degli obiettivi fissati, fino a compromettere la stabilità dell'intera struttura. Un chiaro esempio in tal senso è fornito dal rischio reputazionale, rispetto al quale assume maggiore interesse la perdita di fiducia che il pubblico accorda all'impresa; mentre il guadagno di consensi è interpretato come la conseguenza che testimonia la bontà delle scelte intraprese e per il quale ci si limita alla constatazione del risultato, diversamente accade per la perdita

di reputazione rispetto alla quale la direzione deve immediatamente correre ai ripari. Tale rischio – aggravato dalla difficoltà di valutazione – è in grado di minacciare seriamente la sopravvivenza dell'intermediario. Nella maggior parte dei casi è però possibile pervenire ad una stima di massima dell'esposizione attraverso l'analisi delle componenti di frequenza ed impatto. La frequenza esprime con quale assiduità – sulla base di calcoli statistici che originano dai dati storici – l'evento è in grado di manifestarsi. L'impatto è invece l'onerosità[23] che l'intermediario dovrà sopportare qualora la minaccia dovesse trovare riscontro pratico.

La combinazione di tali elementi fornisce la misura dell'evento rischioso e così accade per tutti i riscontri che la mappatura dei rischi porta in evidenza. Di fronte al manifestarsi di tali eventualità avverse il CoSO Report ha individuato distinte modalità di approccio adottabili dal management:

- l'evitare alcun tipo di assunzione del rischio, anche parziale, scegliendo di non cogliere l'opportunità direttamente connessa all'evento negativo;
- la riduzione, attraverso la predisposizioni di idonee misure volte alla prevenzione piuttosto che all'abbattimento della manifestazione e dell'impatto dello stesso;
- la condivisione, attraverso la stipula di contratti assicurativi o il trasferimento dell'eventuale manifestazione negativa a terzi;
- l'accettazione, semplicemente ponendosi in modo passivo senza intraprendere alcun tipo di operazione che possa in qualsiasi modo ridurne le conseguenze.

Detti esempi di condotta sono espressione delle scelte che l'alta direzione può operare nel momento di definizione degli obiettivi e di conseguenza dei rischi ad essi direttamente legati.

[23] Poiché come detto il management è interessato agli aspetti negativi degli eventi aleatori.

La scelta dell'approccio spetta tuttavia solo all'organo gestorio, l'unico in condizione di assumersene la responsabilità, poiché soggetto chiamato a definire le strategie volte al raggiungimento dei risultati stabiliti. È dunque opportuno, nella definizione di una politica di rischio, individuare in via preliminare i traguardi che l'entità si prefigge di raggiungere, indagandoli a fondo e rendendoli stabili.

Solo attraverso il successo di tale operazione preliminare è possibile realizzare i passi successivi che prevedono la mappatura dei rischi che interessano l'azienda bancaria e le relative azioni volte ad eliminarli, o quantomeno a diminuirne l'influenza.

Quanto alla mappatura dei rischi essa consiste nell'esame preliminare di tutti i fattori che possono comportare un ostacolo, una volta definiti gli obiettivi che l'azienda intende raggiungere.

Si tratta, come detto, di un'attività preliminare imprescindibile, sulla quale basare la realizzazione delle fasi successive di creazione della cultura aziendale e definizione della politica di rischio, assegnazione delle funzioni di controllo all'interno della struttura, predisposizione di adeguati flussi informativi, gestione del rischio e revisione periodica del sistema. Attraverso tale fase preliminare l'alta direzione è in grado di assumere decisioni in merito all'approccio da adottare nei confronti dei rilievi, mentre spetterà agli altri soggetti destinatari di funzioni di controllo – in coordinamento con gli organi direttivi – fornire la valutazione degli elementi rischiosi e monitorarli lungo l'arco temporale in cui l'attività bancaria si svolge.

La stessa Autorità di Vigilanza si è pronunciata sul tema sottolineando la necessità da parte del Sistema dei Controlli Interni di sviluppare una conoscenza approfondita in merito a tutte le tipologie di rischio che possono interessare l'organizzazione, valutandone l'esposizione attraverso

metodologie di misurazione per le fattispecie che ne consentono la quantificazione.

Al fine di realizzare una corretta mappatura di tutti i rischi è necessaria l'indagine completa dei processi aziendali attraverso i quali si realizza l'attività e la correlazione di questi ultimi alle rispettive manifestazioni di rischio che potrebbero interessarli.

Per tali ragioni è necessaria la chiara conoscenza degli obiettivi che il management ha posto ed allo stesso tempo devono essere compresi i processi attraverso i quali realizzarli. Solo in questo modo è possibile ottenere una conoscenza completa delle minacce all'attività bancaria che permetta l'agire informato e la conseguente adozione di soluzioni di contrasto efficaci.

A compimento dei cenni in materia di rischi che l'impresa bancaria deve necessariamente affrontare per il raggiungimento del successo aziendale, è necessaria l'individuazione delle categorie nelle quali le minacce vengono suddivise.

Nella letteratura sul tema sono numerose le fonti che propongono una propria suddivisione dei rischi, seguendo metodologie di riclassificazione personali, ma tuttavia si ritiene di maggiore utilità fare riferimento alle "Nuove disposizioni di vigilanza prudenziale" emesse da Banca d'Italia nel 2006. La ripartizione operata nel testo è finalizzata alla determinazione del patrimonio di vigilanza per mezzo del processo ICAAP – Internal Capital Adequacy Assessment Process.

Tale metodo di valutazione è volto alla determinazione di un livello di patrimonio "prudenziale" del quale il singolo istituto deve dotarsi per poter fronteggiare le conseguenze negative della manifestazione dei rischi dai quali è afflitto. Attraverso la misurazione dell'impatto di tali eventi avversi per mezzo di metodologie di calcolo differenti, l'intermediario è in grado di

definire un livello di patrimonio che possa garantire una certa stabilità, quantomeno rispetto alle tipologie di rischio valutabili. Nel Capitolo 1 del Titolo III delle citate disposizioni è possibile leggere che "le banche effettuano in autonomia un'accurata identificazione dei rischi ai quali sono esposte, avuto riguardo alla propria operatività e ai mercati di riferimento" e "ai fini della determinazione del capitale interno, le banche misurano ovvero – in caso di rischi difficilmente quantificabili – valutano tutti i rischi rilevanti ai quali sono esposte, utilizzando le metodologie che ritengono più appropriate, in relazione alle proprie caratteristiche operative e organizzative".

Per quanto riguarda le categorie di rischio rilevanti "l'analisi deve considerare almeno i rischi contenuti nell'elenco di cui all'Allegato A. Detto elenco non ha carattere esaustivo: è rimessa alla prudente valutazione di ogni banca l'individuazione di eventuali ulteriori fattori di rischio connessi con la propria specifica operatività".

Il contenuto dell'allegato in questione fa riferimento alle seguenti tipologie.

Rischi compresi nel Primo Pilastro:

- Rischio di credito: è originato dall'eventualità di insolvenza o dalle difficoltà a far fronte ai propri impegni, manifestate dalle controparti della banca in operazioni di concessione di finanziamenti.
- Rischio di controparte: è compreso nel rischio di credito e riguarda la possibilità che la controparte risulti inadempiente al momento del regolamento finale dei flussi finanziari di un'operazione.
- Rischio di mercato: è originato dalle conseguenze avverse di movimentazioni di capitali sui mercati finanziari in cui opera l'istituto. Esso comprende il rischio di posizione generico su titoli di debito, il rischio di posizione generico su titoli di capitale, il rischio di posizione specifico su titoli di capitale, il rischio di concentrazione

del portafoglio di negoziazione, il rischio di regolamento, il rischio di cambio, il rischio di posizione in merci.

- Rischio operativo: trae origine dall'inadeguatezza o dall'inefficacia di procedure, risorse umane, unità interne o eventi esterni avversi alla gestione dell'ente ed in grado di comportare perdite di risorse finanziarie. Sono ad esso riconducibili le frodi, gli oneri derivanti da errori umani, nonché perdite contrattuali e catastrofi naturali. Allo stesso modo è compreso il rischio legale, ma non quello strategico.

Altre tipologie di rischio:

- Rischio di concentrazione: deriva da esposizioni eccessivamente rivolte nei confronti di medesime controparti, soggetti appartenenti allo stesso gruppo, nonché appartenenti al medesimo settore industriale o area geografica.
- Rischio di tasso d'interesse: deriva dalla variabilità connessa ad attività diverse dalla negoziazione in relazione al mutamento dei tassi di interesse.
- Rischio di liquidità: si manifesta sotto forma di incapacità da parte dell'intermediario di onorare tempestivamente i propri impegni di cassa, sia sotto forma di incapacità di reperire i fondi (funding liquidity risk), che di limitazioni allo smobilizzo delle attività finanziarie detenute (market liquidity risk).
- Rischio residuo: è costituito dalla minaccia che i processi e le procedure istituite per la mitigazione del rischio di credito disattendano le aspettative di performance previste.
- Rischio da cartolarizzazioni: deriva dall'eventualità che la sostanza economica dell'operazione di cartolarizzazione non sia pienamente rispecchiata nelle decisioni di valutazione e di gestione del rischio.
- Rischio strategico: si manifesta attraverso riduzioni attuali o future dei risultati economici o del capitale dell'ente in conseguenza di

scelte aziendali errate, attuazione inadeguata delle scelte, cambiamento del contesto operativo e conseguente mancato adeguamento alle condizioni.

- Rischio reputazionale: è la manifestazione di riduzioni attuali o future dei risultati economici o del capitale dovute ad una percezione negativa dell'immagine dell'istituto da parte della clientela, delle controparti, degli azionisti, degli investitori, nonché delle autorità di vigilanza.

L'autorità di vigilanza, sebbene sottolinei la non esaustività delle fattispecie di rischio contenute nell'elenco esposto, raccomanda di fare riferimento ad esso anche al di fuori delle valutazioni finalizzate alla determinazione del patrimonio di vigilanza, in modo tale da mantenere la coerenza tra rischi rilevati e metodologie di valutazione.

2 LA FUNZIONE DI COMPLIANCE

2.1 Definizione e funzioni dell'attività di compliance

Le leggi riflettono i bisogni ed i valori attuali della società; di conseguenza, la regolamentazione è una risposta, poiché raramente può anticipare o immaginare le problematiche future, e ancora oggi richiede la definizione del problema e l'identificazione di potenziali risoluzioni. In ambito internazionale, la giurisprudenza non è l'unica forma di controllo sociale o di rivendicazione normativa. Altre disposizioni comportamentali emergono dalla moralità, dalla cortesia e dalle consuetudini sociali, che costituiscono parte delle aspettative sociali.

Nella letteratura sulla regolamentazione, il termine "compliance" assume due accezioni: quella principale verte sulle popolazioni di riferimento della regolamentazione, sui limiti entro cui queste vi si conformano e le loro motivazioni; la seconda è nata da un approfondimento sugli enti regolatori, sul genere di strategie applicative normative impiegate e da impiegarsi.

Nel secondo caso, il termine compliance ha assunto un significato specialistico, alquanto in contrasto con il primo, che guarda all'approccio regolatore, piuttosto che alla risposta delle popolazioni di riferimento. Si tratta di un approccio regolatore particolare che vuole garantire la compliance, contando soprattutto sulla persuasione e cooperazione, anziché sulle sanzioni e pene legali.

Invece nel primo caso, la compliance definisce l'aspetto cooperativo e persuasivo dell'attuazione regolamentare che, in quanto modello normativo, la pone a confronto con l'approccio deterrente, il quale presuppone che le imprese operino secondo i proprio interessi. Fin quando le aziende avranno come obiettivo principale la massimizzazione del profitto, non potranno che

essere degli amorali calcolatori, rispettosi delle regole solo se le pene saranno abbastanza pesanti per cui converrà evitarle, guardando alla compliance come al risultato di un'equazione tra i benefici della "non-compliance" e la possibilità di venire scoperti e puniti, in maniera severa. Nel complesso, si presume che le motivazioni fornite dal metodo deterrente sono il timore della pena, piuttosto che il calcolo razionale dell'onere potenziale delle pene e delle sanzioni.

Studiosi di legge ed economia assumono che tale approccio funzionerà solo in presenza di ristrette circostanze: le aziende rivelano un'assoluta tendenza alla massimizzazione del profitto; la giurisprudenza stabilisce senza ambiguità i comportamenti scorretti; le pene legali forniscono l'incentivo primario alla compliance aziendale; gli organismi esecutivi scoprono e puniscono i comportamenti scorretti, utilizzando le risorse disponibili. Perlopiù queste premesse non sono sempre valide, quindi un semplice modello deterrente non è molto utile per spiegare cosa spinge le imprese a rispettare la legge, e questo sia perché gli enti regolatori non sono così potenti ed efficienti come invece dovrebbero essere per far funzionare l'approccio deterrente, sia perché vista l'alta remunerazione e l'irrilevante penalizzazione di così tanti tipi di violazioni aziendali, l'aspetto minatorio delle sanzioni non è abbastanza grave per distogliere dalla non-compliance. Questo perché le conseguenze economiche della non-compliance, che non attirano l'attenzione su di se generando un qualche tipo di crisi, vengono spesso trascurate da un management troppo occupato. L'imposizione di pene consegue un miglioramento per la sicurezza delle imprese, in quanto attira l'attenzione del management sul rischio che altrimenti sarebbe stato trascurato. Solitamente, la razionalità limitata delle imprese e del top management – cioè la capacità limitata delle persone e delle aziende nel trattare informazioni nel corso di un processo decisionale – si riferisce al fatto che in molti non valutano affatto la redditività razionale relativa alla

compliance. Solo nel caso in cui accadesse qualcosa che attiri l'attenzione sul rischio della non-compliance, l'approccio deterrente diverrebbe reale. Nell'eventualità di un disastro di natura politica o economica, o qualora le aziende fossero abbastanza grandi, affermate, altamente individuabili e quindi attente alla loro pubblica immagine, solo allora sarebbe possibile un approccio di tipo deterrente.

Molte aziende sono incentivate a rispettare la legge, o ad apparire conformi ad essa, così da conservare agli occhi del governo, del mercato e del pubblico una certa legittimità.

Nel campo economico si cerca di attestare che gli individui e le aziende non prendano decisioni sempre ed unicamente sulla base di calcoli finanziari, ma considerino anche una varietà di altri fattori sociali ed ambientali, compresi i loro valori e le aspettative altrui che ne influenzeranno le azioni.

Edwards e Wolfe definiscono la compliance nel seguente modo: «Compliance in general terms is the adherence by the regulated to rules and regulations laid down by those in authority. Not only does compliance means adherence to the letter of the law it also is just as concerned with adherence to the spirit of the law»[24]1, pertanto, il termine "Compliance" «includes concepts of obedience, observance, deference, governability, amenability, passivity, no-resistence and submission», coniugando "a rules-based approach to a more flexible athical one".

Tale definizione è analoga a quella proposta dalla Banca d'Italia, nel documento di consultazione sulla compliance[25], dal quale si evince la volontà di «promuovere una cultura aziendale (...) orientata al rispetto, non solo della lettera, ma anche dello spirito delle norme», attraverso l'istituzione di una funzione apposita di prevenzione e gestione del rischio

[24] Edwards J. (2003)
[25] Banca d'Italia (2006).

di non conformità, vale a dire del «rischio di incorrere in sanzioni giudiziarie o amministrative, perdite finanziarie rilevanti o danni di reputazione in conseguenza di violazioni di norme di legge, di regolamenti, ovvero di norme di autoregolamentazione o di codici di condotta».

Secondo la definizione di Edwards e Wolfe la compliance rappresenta la chiave operativa e reputazionale dell'intero sistema dei servizi finanziari; essa è saldamente coinvolta nel processo con il quale le organizzazioni finanziarie eseguono l'intera attività di investimento. Dello stesso parere anche Hagland[26], il quale ritiene che l'attività di compliance debba garantire l'osservanza delle norme e dei regolamenti ai quali ogni impresa è sottoposta. Egli in particolare asserisce che "compliance is about the protection of the client: managing one's business as to ensure, as a minimum, that it is conducted in accordance with the law".

L'attività di compliance, così come definita, deve essere inserita e analizzata nel contesto evolutivo della regolamentazione, che ha fatto seguito agli eventi di fallimento del mercato verificatisi, in maniera largamente diffusa, nell'intero sistema finanziario nel corso dell'ultimo decennio. Il risultato di questi accadimenti, che hanno coinvolto milioni di

risparmiatori, dipendenti e stakeholder, è stato l'aumento dell'attenzione, da parte delle autorità di vigilanza per la promozione e il sostegno di comportamenti etici e conformi alle regole.

A testimonianza di questa atmosfera di cambiamento si è assistito all'aumento dei tassi di adozione di codici etici e di programmi di compliance legale. Richardson[27]4 afferma che oggi tutte le maggiori aziende hanno adottato codici etici e istituito dipartimenti o assegnato responsabilità a specifiche personalità per la gestione dei rischi inerenti

[26] Hagland G. (1994).
[27] Richardson S. M., McNamara Hilmer K., Courtney J. F. (2005), p. 1.

l'etica aziendale. A fronte di questi cambiamenti, certamente significativi, tuttavia, Weaver[28]5, fa notare che esiste una ampia variabilità delle modalità di applicazione dei programmi etici e delle strutture adibite alla verifica della conformità delle attività quotidiane alle policy interne; in effetti si riscontra che la gran parte delle imprese ha adottato un codice etico perché ritiene che queste forme di garanzia dell'integrità aziendale siano quelle che coniugano un basso costo con un elevato impatto simbolico.

Il legame fra l'etica e la compliance viene più volte sottolineato e studiato da numerosi altri autori[29]6, i quali sottolineano l'importanza di affiancare ai programmi di compliance un solido orientamento ai comportamenti etici, dimostrando che "the objective of responsible conduct cannot be achieved solely by imposing from outside what is required but must also appeal to what is desired"[30].

Il successo di un programma di compliance orientato all'etica dipende, secondo Weaver e Trevino[31]8, da due fattori in particolare: dalla struttura dei programmi e dal contesto, unico in ogni organizzazione, in cui il programma stesso è applicato. Inoltre, come suggerito da una ulteriore ricerca compiuta dai due autori[32], la compliance alle policy è influenzata anche dalla percezione soggettiva e individuale dei due fattori citati.

Con specifico riferimento alla tipologia dei programmi adottati dalle aziende, la letteratura[33] distingue due principali modelli, costruiti secondo differenti obiettivi e orientamenti: un compliance-based approach e un integrity or value-based approach.

---

[28] Weaver G. R., Trevino L. K., Cochran P. L. (1999).
[29] Fra i principali si possono citare: Paine L. (1994); Laufer W. S., Robertson D. C. (1997); Trevino L. k.,Weaver G. R., Gibson D. G., Toffler B. L. (1999); Weaver G. R., Trevino L. K. (1999) e (2001); Jackman D. (2001); Edwards J., Wolfe S. (2005); Weber J., Fortun D. (2005); Michaelson C. (2006).
[30] Michaelson C. (2006).
[31] Cfr. Weaver G. R., Trevino L. K. (1999).
[32] Weaver G. R., Trevino L. K. (2001).
[33] Paine L. S. (1994), Weaver G. R., Trevino L. K. (1999).

Il primo è principalmente focalizzato sulla prevenzione, il controllo e la punizione dei responsabili delle violazioni rilevate; mentre il secondo persegue lo scopo di definire chiaramente i valori dell'organizzazione e incoraggiare l'atteggiamento dei dipendenti verso aspirazioni etiche e verso lo sviluppo di valori etici condivisi.

Weaver e Trevino hanno esaminato le relazioni fra i due metodi, soffermandosi in particolare sull'influenza che questi esercitano sui comportamenti e la propensione degli impiegati.

Essi ritengono che i due approcci non sono alternativi fra loro e che la percezione di un impiegato riguardo all'orientamento dei programmi etici aziendali è importante nel determinarne i comportamenti. Senza una direzione comune e chiaramente individuata ognuno può percepire differenti valori e orientamenti alla compliance, perché influenzato dal proprio contesto organizzativo; anche nella circostanza in cui ci fosse la volontà da parte del management di adottare un programma etico con caratteristiche uniformi nell'intera organizzazione, questo potrebbe, pertanto, essere interpretato e implementato in maniera diversa "by different people in different places". Tutto ciò premesso, gli autori suggeriscono di non adottare programmi orientati al mero rispetto delle regole, ma di perseguire la creazione di "a sense of shared values that can help define an ethical role for individuals", una combinazione di "compliance and values approaches is ideal"[34].

Jackman, in particolare, propone lo sviluppo dei valori etici e della cultura della compliance sia nelle organizzazioni, sia a sostegno dell'attività

[34] In una indagine compiuta dalla Ethics Officers Association (EOA) nel 2000 presso circa 150 organizzazioni, appartenenti a diversi settori economici e di dimensioni variabili, tutte aderenti all'associazione, dimostra che al responsabile dell'applicazione di programmi etici e di compliance sono stati attribuiti circa 100 titoli diversi. In questi titoli la parola "ethics" si presenta con una frequenza del 35%, mentre il termine "compliance" ha una frequenza del 37% circa. Indagini successive, tra cui quella di Weber e Fortun, seppure su un campione di riferimento sensibilmente ridotto (14 aziende), il temine "compliance" ha una frequenza dell'85%, mentre "ethics" si presenta con una frequenza del 21,4%. Cfr.: Weber J., Fortune D. (2005), p. 102.

dell'autorità di vigilanza; riconoscendo l'importanza di un cambiamento che coinvolga nel complesso l'intero sistema finanziario[35]. Mentre, infatti, inizialmente si poteva essere indotti a pensare che la domanda di comportamenti compliant fosse indirizzata nei confronti del singolo individuo, la tendenza che si è sviluppata col passare del tempo, è stata quella di estendere i concetti di compliance competence and ethics alle intere organizzazioni.

Le autorità di vigilanza (per esempio la FSA e la Banca d'Italia), in questa ottica, attribuiscono ai senior manager il compito di istituire e mantenere un appropriato sistema di controlli, al fine di assicurare che ogni individuo agisca con integrità e con la dovuta diligenza, in accordo a quanto stabilito da appropriate policy interne. «It is only if this is happening that it can be said that the organisation is operating in a compliance competent manner»[36].

Poiché, inoltre, un cambiamento non può essere forzato, il ruolo dell'autorità di vigilanza è di fondamentale importanza; essa deve essere d'ausilio alle imprese nel formare una cultura aziendale che induca ogni individuo a passare dalla mera conformità alle regole, ad una piena consapevolezza del significato e dello "spirito" delle norme stesse. Questa forma di regolamentazione si contrappone a quella "reactive to events and external influences" e può, pertanto, essere definita " proactive".

I nuovi approcci regolamentari sollecitati dal Comitato di Basilea, riconoscono i limiti di un sistema guidato da principi di rule-based compliance e tentano di sviluppare un approccio meno prescrittivo alla compliance, incoraggiando gli intermediari finanziari ad articolare i propri valori e il proprio credo nell'ambito di un contesto etico, in collaborazione

[35] «It is this integration that Jackman's model of development of organisational values and culture seeks to identify and encourage in a compliance competent organisation» Edwards J., Wolfe S. (2005).
[36] Jackman D. (2001).

con le autorità di vigilanza. In questa ottica deve essere valutata anche la libertà nell'applicazione del modello organizzativo riconosciuta dalla Banca d'Italia nel suo documento di consultazione, in applicazione delle prescrizioni del Comitato di Basilea.

La compliance è, evidentemente, un fenomeno complesso, che si inserisce fra il concetto di rischio e di regolamentazione: "regulation is both a form of risk management and a source of compliance risk. As regulation seeks to operate increasingly with the grain of organisational life, risk management in its broadest sense represents the continuation of regulatory programmes with businesses. Accordingly, the inside of the organisation is increasingly recognised as a "regulatory space" in which the various facets of compliance are determined"[37].

2.2 Il rischio di compliance e la cultura aziendale

La funzione di compliance è posta a presidio del rischio di non conformità, definito dal Comitato di Basilea[38] come il "rischio di sanzioni legali e di perdite finanziarie o di reputazione, che la banca potrebbe soffrire come risultato del fallimento della conformità a leggi, regole, standard di autoregolamentazione e codici di condotta applicabili alle attività bancarie". Come evidente, si tratta di un rischio che comprende aspetti fortemente eterogenei, coinvolgendo sia elementi tipici del rischio legale che del rischio operativo e reputazionale.

La difficoltà principale nella gestione del rischio di conformità nasce, appunto, da questa complessità di definizione, che comporta la possibilità di creare sovrapposizioni e sprechi di risorse rispetto ai presidi già esistenti, impiegati nella gestione e nella misurazione delle altre tipologie di rischio. Il Comitato di Basilea definisce il rischio operativo come "il rischio di

[37] Hutter B., Power M. (2000), p. 4.
[38] Comitato di Basilea (2005).

perdite derivanti dalla inadeguatezza o dalla disfunzione di procedure, risorse umane e sistemi interni, oppure da eventi di origine esogena"; lo stesso Comitato asserisce che la definizione appena citata include i rischi legali, ma esclude volontariamente i rischi strategici e di reputazione[39].

I rischi operativi sono "rischi puri", vale a dire che da una loro eventuale manifestazione possono generasi solo perdite e mai opportunità di profitto, in ciò si differenziano in maniera sostanziale rispetto ai rischi finanziari, che vengono, infatti, definiti anche "rischi speculativi".

Sia i rischi operativi che i rischi di compliance originano, a ben vedere, dal mancato o inefficiente presidio di alcuni ambiti di operatività aziendale e le definizioni proposte delineano un'area di sovrapposizione fra le due tipologie di rischio[40].

Lo stesso Comitato di Basilea[41] afferma che "there is a close relationship between compliance risk and certain aspects of operational risk", per questo motivo riconosce che "some banks may wish to organise their compliance function within their operational risk function", mentre altre possono decidere di istituire un organismo per l'attività di compliance indipendente dalla funzione di operational risk management "but establish mechanisms requiring close cooperation between the two functions on compliance matters".

Secondo la formulazione di rischio legale adottata dal Comitato di Basilea tale tipologia "comprede, fra l'altro, l'esposizione ad ammende, sanzioni pecuniarie o penalizzazioni derivanti da provvedimenti assunti dall'organo di vigilanza, ovvero da regolamenti privati"[42].

[39] Comitato di Basilea (2004).
[40] Uselli A. (2005).
[41] Comitato di Basilea (2005), p. 8.
[42] Comitato di Basilea (2004), p. 120.

Anche questa definizione ha elementi comuni sia al compliance risk, che al rischio operativo, se si pensa, in particolare, alle perdite monetarie dovute al mancato assolvimento di obblighi legislativi, con conseguenti esborsi dovuti all'accertamento delle responsabilità a carico dell'intermediario, oppure alle perdite derivanti da condotta impropria nei confronti di terzi, che possono generare risarcimenti anche volontari da parte della banca[43].

Cola[44] definisce il rischio legale nel seguente modo: "rischio di perdita o riduzione di valore delle attività di portafoglio, a causa di contratti o documenti legali inadeguati o non corretti o contenenti clausole che si rivelino particolarmente onerose". La definizione individua, dunque, una fattispecie di rischio più circoscritta rispetto a quello di non conformità, che, invece, coinvolge aspetti di tipo reputazionale e inerenti la presenza di possibili conflitti d'interesse.

Il rischio reputazionale si sostanzia nella possibilità del verificarsi di danni economici derivanti dall'alterazione del giudizio e del rapporto fiduciario percepito dalla clientela dell'intermediario[45]. E' evidente che questa tipologia di rischio è particolarmente rilevante per il sistema bancario, in cui il rapporto fiduciario con la clientela rappresenta l'elemento qualificante dell'esistenza stessa dell'intermediazione creditizia.

Data la manifesta "intangibilità" del requisito reputazionale, anche la valutazione del rischio ad esso associato diventa problematica, tanto più se si riflette sulla specificità della tipologia di eventi che caratterizzano la sfera reputazionale, in considerazione del fatto che da essa possono derivare "perdite assolutamente sproporzionate rispetto all'evento originario"[46]23.

[43] Uselli A. (2005), p. 330.
[44] Cola C. (2005).
[45] Gabbi G. (2003), p. 1.
[46] Gabbi G. (2003), p. 3.

Allegrini[47]24 afferma che "quanto più l'azienda (…) fa affidamento a valori immateriali quali l'immagine, la fiducia e la creatività, tanto maggiore sarà l'entità del danno. Così i danni saranno presumibilmente più consistenti per le aziende che offrono un prodotto o un servizio ad elevata "personalizzazione", in cui la forza del marchio o dell'immagine aziendale risultano determinanti".

Il Comitato di Basilea propone, in merito, la seguente definizione: "reputational risk arises from operational failures, failure to comply with relevant laws and regulations, or other sources. Reputational risk is particularly damaging for banks since the nature of their business requires maintaining the confidence of depositors creditors and the general marketplace".

Il rischio reputazionale è scatenato da fattori di rischio originari, quali il rischio operativo, il rischio legale e strategico, tuttavia, l'individuazione e la misurazione di queste tipologie di rischio non sono sufficienti all'analisi del problema, perché affinché gli eventi operativi, legali e strategici condizionino la reputazione di un soggetto è necessario che si verifichino ulteriori condizioni[48]:

1. la diretta responsabilità dell'impresa o di un suo soggetto nell'adozione di scelte con effetti negativi per la reputazione;

2. l'attivazione di specifiche variabili (reputazionali) che contribuiscono alla trasformazione del rischio originario in un fattore in grado di modificare il giudizio interno ed esterno dell'impresa.

In merito alla definizione di rischio operativo e di compliance, Uselli propone una riflessione interessante, affermando che dalla mappatura dei rischi operativi si evince che essi sono prevalentemente di natura

[47] Allegrini M. (2000).
[48] Gabbi G. (2003), p. 4

"inconsapevole": si tratta cioè di eventi che si manifestano in maniera indipendente rispetto alle decisioni aziendali, sia perché ricollegabili a fattori di rischio esterni, in relazione ai quali è minore il controllo esercitabile dall'intermediario, sia perché inevitabilmente ricollegabili alla natura stessa del rischio d'impresa. Al contrario il compliance risk è, in prevalenza, originato da scelte consapevoli, concretizzabili nel mancato rispetto della normativa esterna o interna.

Una indagine compiuta dalla PricewaterhouseCoopers[49] ha dimostrato che non c'è un consenso generalizzato sulla definizione di compliance risk, di operational risk e reputational risk. Le principali differenze sono dovute al diverso livello evolutivo dell'approccio al risk management e della funzione compliance, dal posizionamento organizzativo dell'unità di compliance all'interno dell'azienda, dalla recettività culturale dimostrata dall'impresa nei confronti della regolamentazione.

La necessità che si ravvisa è quella di avere un linguaggio e un approccio comune alla compliance e, in questa ottica, un contributo importante può essere fornito dal Comitato di Basilea, che dovrebbe contribuire ad aumentare la chiarezza riguardo al ruolo e alla responsabilità della funzione di conformità e agevolare l'uniformazione dei diversi riferimenti regolamentari interni agli intermediari.

Il rischio di compliance, come tutti i rischi, può essere affrontato o incidendo sulla probabilità di accadimento (la cultura aziendale) o sugli effetti derivanti dal verificarsi dell'evento dannoso; la prima ipotesi consiste nel motivare opportunamente le proprie risorse umane e favorire la loro adesione agli obiettivi ideali dell'azienda; mentre, la seconda ipotesi è relativa alla capacità dell'azienda di fronteggiare le conseguenze

[49] PricewaterhouseCoopers (2005), p. 16. L'indagine è stata compiuta, durante la seconda metà del 2004, su un campione di 73 intermediari finanziari (prevalentemente bancari, 63% del campione di riferimento), appartenenti a 17 paesi diversi fra Asia e Australia, Nord America, Europa e Medio Oriente.

dell'evento una volta verificatosi; tale capacità dipenderà dai meccanismi di contenimento dei danni economici e reputazionali attuati mediante le opportune tecniche di gestione e ritenzione del rischio.

In questo caso, tuttavia, il sapiente utilizzo di riserve o strumenti esterni, come le assicurazioni, non è sufficiente a contenerne gli effetti, essendo il danno reputazionale, coinvolto nel processo di compliance, caratterizzato non solo da una componente di danno economico immediato, ma anche foriero di effetti futuri difficilmente quantificabili. Se ne deduce come, al fine di gestire adeguatamente il rischio di non conformità, sia essenziale e prioritaria la formazione di una cultura Compliant-oriented. Langevoort[50] afferma, a tal proposito, che «Compliance begins with education», attraverso un efficace processo di comunicazione e formazione, tale che i soggetti interni all'impresa comprendano l'orientamento dell'azienda e sappiano quali comportamenti ci si attende da loro.

Dello stesso parere la Schwizer che sul tema afferma: «la compliance non può essere tale senza una base culturale che consideri il rispetto delle norme come un valore primario cui l'azienda e il comportamento di tutti i suoi attori devono ispirarsi». E' necessario, dunque, verificare che esista una cultura aziendale e una coerente azione manageriale che sostengano l'attività di gestione del rischio di compliance[51].

A tal proposito uno studio compiuto da Trevino[52] dimostra come specifiche caratteristiche possono influenzare il successo di programmi etici o di compliance alle norme e fornisce solide evidenze riguardo a ciò che deve essere fatto e ciò che invece deve essere evitato affinché si compia un efficace sistema di ethic/compliance management. Fra le caratteristiche che hanno dimostrato un'incidenza positiva ne vengono segnalate cinque: la

[50] Langevoort D. C. (2001).
[51] Schwizer P. (2006). Inoltre Cfr. Schwizer P. (2006b).
[52] Trevino L. K., Weaver G. R., Gibson D. G., Toffler B. L. (1999).

coerenza fra le strategie politiche e l'agire quotidiano; il grado di diffusione di una cultura orientata all'etica e alla compliance; la presenza di una "ethical leadership"; il trattamento equo degli impiegati; la volontà di promuovere confronti e discussioni periodiche sull'etica all'interno dell'azienda. Al contrario, ciò che risulta essere in conflitto con il successo di un programma orientato all'etica e alla compliance, è una cultura che enfatizza gli interessi particolaristici e un'obbedienza incondizionata alle autorità, nonché la percezione che tali programmi siano stati predisposti con il solo obiettivo di proteggere il top management da eventuali colpe o responsabilità. Anche la Banca d'Italia, ribadendo l'importanza della legalità e della correttezza negli affari, in particolare nell'attività bancaria, e riconoscendo che la maggiore complessità dell'attività bancaria rende più complicato identificare ed esercitare un controllo sui comportamenti che possono costituire violazione delle norme, degli standard operativi, dei principi deontologici ed etici dell'attività di intermediazione, richiama l'attenzione sulla necessità, da un lato, di "promuovere una cultura aziendale improntata a principi di onestà, correttezza" e, dall'altro, di predisporre "specifici presidi organizzativi, volti ad assicurare il rigoroso rispetto delle prescrizioni normative e di autoregolamentazione"[53]. L'indagine compiuta dalla PriceWaterHouse&Coopers[54] nel 2005, confermando questo orientamento, riporta testualmente che: «A coherent, ongoing strategy for the compliance function has two dimension, operating against the backdrop of comprehensive awareness of stakeholder expectations and maturity culture of integrity».

[53] Banca d'Italia (2006), Normativa di vigilanza in materia di "conformità alle norme (compliance)", Documento per la consultazione, agosto, p. 2.
[54] PriceWaterHouse&Coopers (2005).

Secondo Hinna[55] introdurre la compliance attraverso una disposizione prescrittiva rischia di "anestetizzare" la crescita spontanea di coscienza aziendale sul tema, che richiede del tempo e non può essere né imposta né acquisita dall'esterno, altrimenti, come suggerisce fra gli altri anche Zamagni[56], si cercheranno le condizioni per il raggiro della norma non appena se ne verifichi l'occasione. Questo è tanto più vero quanto più si predilige un sistema sanzionatorio rispetto ad uno che premi i virtuosi.

A tal proposito, Paine afferma che la "disciplina" è una componente necessaria di ogni sistema etico e compliant e che giuste sanzioni per chi viola le norme sono necessaire ed appropriate, tuttavia, una eccessiva enfasi sul sistema sanzionatorio può dimostrarsi superflua o addirittura controproducente. Egli scrive che «those managers who define ethics as legal compliance are implicity endorsing a code of moral mediocrity for their organizations»[57].

Breeden, ex presidente della Securities Exchange Commission (SEC), ha affermato che "It is not an adequate ethical standard to aspire to get through the day without being indicted". Jackman si chiede, infatti, se la "paura" possa rappresentare il principale elemento che induce le aziende ad essere compliant e, al fine di scongiurare questo atteggiamento, suggerisce un modello, che ha alla base il cambiamento nelle relazioni fra autorità di vigilanza e le società sottoposte all'attività regolamentare. L'indagine riferisce, fra l'altro, che i due principali cambiamenti strettamente interconnessi al raggiungimento della compliance su basi sostenibili sono: "(1) Embedding a compliance culture within the organisation, particularly across borders and across sectors; (2) Remaining compliant on a cross-border, cross-sector basis in the context of a dynamic business environment

[55] Hinna con riferimento alla creazione di un'unità di compliance afferma in maniera ampiamente condivisibile, che: «si può dare in outsourcing la gestione, ma non si può dare in outsourcing la creazione di una nuova cultura aziandale», Hinna L. (2006).
[56] Zamagni S. (2006).
[57] Paine L. S. (1994), op. cit., p.111.

and rapidly changing regulations". Altri autori[58], riguardo alla possibilità di indurre cambiamenti culturali nell'organizzazione aziendale, si chiedono, posto che ciò sia possibile[59], se questi cambiamenti siano dettati da una mera aderenza alle norme, vale a dire che essi producono alterazioni solo nei "material manifestations and behaviours", oppure anche nei valori condivisi dal personale.

Gli studi di Ogbonna e Harris, focalizzati su un caso aziendale, dimostrano che gli sforzi profusi per indurre cambiamenti culturali all'interno dell'organizzazione producono impatti diversi: cambiamenti materiali frequenti e limitati effetti sui valori aziendali. Willmott[60] afferma che il controllo sulla cultura aziendale è "a medium of domination, the scope and penetration of management control". Con l'aumento della complessità organizzativa e gestionale e il proliferare delle tecnologie utilizzate all'interno delle aziende si rende necessaria anche un cambiamento nelle strategie di controllo: dai costosi e spesso inefficienti metodi di controllo indirizzati alle strutture o ai processi, alle tecniche di cultural control.

I diversi atteggiamenti presenti in letteratura riguardo alla possibilità di gestire o meno la cultura aziendale sono in primo luogo riconducibili alle differenti definizioni di cultura da cui ogni ricercatore parte, ma in ogni caso è comune il pensare che la gestione della cultura sia più complessa di quella di altre variabili organizzative proprio perché essa "può essere

[58] Ogbonna E., Harris L. C. (1998).

[59] La letteratura che si è occupata di valutare i cambiamenti culturali può essere distinta in due aggregati: 1) analisi di cambiamenti culturali avvenuti naturalmente; 2) studi relativi alla gestione della cultura aziendale, incentrati sull'azione del management. Alla prima categoria appartengono le ricerche compiute ad esempio da Sathe V. (1983); Harrison J. R. e Carrol G. R. (1991). La seconda categoria può essere ulteriormente suddivisa in: a) ricerche in base alle quali la cultura può essere gestita; b) ricerche in base alle quali la cultura può essere manipolata sotto specifiche condizioni; c) studi secondo i quali, seppure sia ritenuto possibile cambiare la cultura di un'organizzazione, la direzione, l'impatto e la sostenibilità del cambiamento non sono variabili soggette all'azione consapevole del management. Fra coloro i quali hanno approfondito queste tematiche si possono citare: a) Bate P. (1994); Brown A. (1995); Dawson P. (1994); Silverzweig S., Allen R. F. (1976); b) Smircich L. (1983); c) Ackroyd S., Crowdy P. (1990); Anthony P. D. (1990); Ogbonna E. (1993); Willmott H. (1993).

[60] Willmott H. (1993), p. 522.

estremamente efficace e, nel contempo, resistente rispetto alle esigenze di cambiamento dettate dai mutamenti nel contesto ambientale"[61].

In merito alla definizione di "cultura aziendale", Carretta propone, in maniera semplice ed efficace, la seguente definizione: «la cultura è quello che si fa e come lo si fa quando non ci si pensa».

L'attività di compliance è un'attività costosa, che comporta ingenti spese iniziali di avviamento e periodici costi di mantenimento, ci si chiede, pertanto, perché sia diventata tanto diffusa fra le imprese. La risposta più ovvia è naturalmente legata all'attività delle autorità di vigilanza, che, dati gli scandali finanziari ricorrenti, hanno puntato ad un maggior rigore regolamentare e a costruire una cultura della legalità e della responsabilità sociale d'impresa; tuttavia si possono rintracciare anche altre motivazioni interne alle aziende stesse che:

- vogliono minimizzare i possibili conflitti con gli stakeholder, che possono rivelarsi assai costosi;
- sperano di incontrare il favore dei clienti, con conseguenze positive sulle vendite, per effetto di una maggiore fiducia;
- comprendono che la produttività del personale dipendente, ben lungi dall'essere meramente determinata da un sistema di punizioni e incentivi monetari, è in larga parte condizionata da motivazioni e finalità ideali elevate perseguite nell'attività d'impresa.

2.3 I requisiti organizzativi della funzione compliance

La letteratura disponibile relativa all'analisi dei requisiti organizzativi della funzione compliance, è prevalentemente riconducibile ad alcune recenti indagini campionarie realizzate negli Stati Uniti d'America e in Europa, il

[61] Carretta A. (2006).

cui obiettivo era quello di mettere in evidenza le principali caratteristiche operative e organizzative della funzione compliance nel sistema finanziario.

L'indagine effettuata dall'American Banking Association (ABA), dal titolo Compliance Watch 2003, ha sviluppato l'analisi della forma organizzativa dell'attività di conformità a partire da una campione di 1.008 banche americane, appartenenti a 49 Stati diversi, e suddivise in classi dimensionali. Ciò che è emerso dall'analisi dei dati è che la forma organizzativa prescelta ed attuata dalle banche americane per istituire una funzione compliance dipende dalla dimensione dell'intermediario. La ricerca indica cinque principali modelli organizzativi fra quelli adottati dalle banche, la cui complessità cresce all'aumentare delle dimensioni dell'azienda bancaria, fra uno di base, in cui la responsabilità della funzione compliance è affidata ad un unico soggetto (modello Stand Alone), che può eventualmente coordinare l'attività svolta in diversi dipartimenti attraverso un referente in loco, e un modello più complesso, in cui troviamo una funzione compliance autonoma e dotata di un proprio staff e di un proprio budget, che, evidentemente, gode anche di maggiore autorevolezza (Divisione autonoma di compliance).

Lo studio in esame, inoltre, ha fornito anche una prima valutazione dei costi di compliance, evidenziando le voci di costo più rilevanti; fra queste, la voce più importante è rappresentata dai salari e dai benefit pagati al personale, a prescindere dalle dimensioni medie delle aziende considerate. Seguono i necessari processi di auditing e monitoring delle attività esposte al rischio di compliance e i costi sostenuti per l'acquisto dei software necessari alla gestione del rischio di non conformità. La spesa per le attività di Infrmation Tecnology cresce in maniera significativa con l'aumentare delle dimensioni medie delle aziende considerate, palesando come, gli ingenti costi che tale attività comporta, possano essere sopportati e risultino strategicamente rilevanti solo per le banche di maggiore dimensione.

Una seconda indagine, compiuta prevelentemente a livello europeo, è stata svolta dalla PriceWaterHouseCoopers nel 2002. La ricerca ha analizzato sia la definizione del rischio di compliance, sia la struttura e l'organizzazione della funzione. Anche in questo caso sono stati individuati tre principali modelli organizzativi, sensibilmente diversi da quelli americani, nonostante presentino analoga nomenclatura.

Il primo modello, definito anch'esso Stand Alone, individua una funzione completamente separata e indipendente dalle altre funzioni aziendali, la cui diffusione è stata rilevata soprattutto in Germania, Olanda, Danimarca, Irlanda, Lussemburgo, Polonia, Svizzera, Regno Unito. Il secondo modello, detto Dependent, è caratterizzato dal fatto che l'attività di compliance è collocata all'interno di un'altra funzione aziendale, in prevalenza l'Internal Auditing, e ha trovato applicazione principalmente in Italia[62] e in Francia; infine, un ultimo modello, definito Deontology, fa riferimento allo schema appositamente introdotto dagli organismi di regolamentazione dei servizi di investimento del mercato finanziario francese, ma l'applicazione non è prevista per le banche.

Lo studio appena citato ha sottolineato, inoltre, la diffusa percezione dell'attività di verifica della conformità come uno strumento di "good corporate governance" e come sia largamente diffusa la necessità di individuare omogenee good practice, nonostante le persistenti differenze nelle forme organizzative prescelte e nelle definizioni di compliance adottate.

Dall'indagine emerge, altresì, come anche i senior manager abbiano capito che la funzione compliance non deve essere un mero strumento per

[62] E' interessante notare che l'indagine in questione considera anche il nostro Paese, basandosi sull'analisi delle istruzioni della Banca d'Italia e della Consob, in cui si fa espresso richiamo alla "attività di controllo interno", ma mai ad una vera e propria attività di compliance, non esistendo ad oggi in Italia un'apposita regolamentazione al riguardo, se si esclude il documento di mera consultazione pubblicato dalla Banca d'Italia lo scorso mese di agosto 2006.

rispondere alle richieste delle autorità regolamentari e di vigilanza, ma deve essere organizzata al fine di aggiunge valore all'azienda e, pertanto, nel rispetto dei requisiti normativi minimi, è necessario cercare di adattare la struttura dell'attività di compliance al proprio modo di fare business. A seguito dell'indagine del 2002 la PricewaterhouseCoopers ha pubblicato altre ricerche sullo stesso argomento, la prima, dal titolo Compliance-A Gap at the heart of risk management, effettuata attraverso un'indagine su 160 istituzioni finanziarie, provenienti dal Nord america, dall'Europa e dall'Asia, presenta l'obiettivo di mettere in luce una nuova consapevolezza della necessità di gestire attivamente il rischio di compliance; il principale elemento di pregio di questo lavoro è l'evidenza data alla mancanza generalizzata di risorse congrue e tra loro coordinate, che spesso ha rappresentato, e rappresenta tutt'oggi, il principale elemento che ostacola l'attività della funzione.

La seconda e più recente indagine[63] ha messo in evidenza come le Autorità regolamentari e di vigilanza stiano accrescendo la propria sensibilizzazione sul ruolo e sulle responsabilità della funzione compliance e come il peso della funzione nelle organizzazioni aziendali sia notevolmente aumentato negli ultimi anni. La ricerca manifesta la necessità di predisporre una compliance più "business oriented", che prediliga il dialogo con la autorità regolamentari e di vigilanza e che promuova l'adozione di una cultura della compliance che pervada l'intera organizzazione aziendale.

La ricerca compiuta negli Stati Uniti da "The Economist Intelligence Unit", i cui risultati sono stati pubblicati di recente, nel marzo 2006, suggerisce di adottare un approccio sistematico nel misurare l'efficacia e i vantaggi dell'attività di compliance; tale criterio consiste nell'analizzare progressivamente la diffusione e la forza della cultura della compliance,

[63] PricewaterhouseCoopers (2005). L'indagine ha coinvolto 73 intermediari, associazioni di settore e autorità regolamentari e di vigilanza in 17 paesi diversi tra Europa, Medio Oriente, Asia, Australia e Nord America.

l'efficacia e l'efficienza dei programmi e il livello di rischio di compliance che l'organizzazione fronteggia. Il lavoro in esame insiste sulla necessità di alimentare una cultura della compliance, attraverso un approccio ampiamente diversificato, basato ad esempio, sull'adozione di codici interni di condotta, di programmi di formazione etici e di un sistema interno di incentivazione del personale basato sul rispetto di comportamenti eticamente corretti; suggerisce, altresì, di controllare e diffondere i canali di comunicazione della compliance, al fine di assicurarsi che ogni persona coinvolta nell'attività sia pienamente consapevole dei rischi che affronta e dei mezzi a sua disposizione per fronteggiarli; rileva, infine, la necessità di destinare congrue risorse per l'identificazione delle aree di rischio emergenti e per lo studio delle regolamentazioni che interessano la propria attività, magari attraverso la formazione di un comitato che mantenga rapporti continuativi con le autorità di vigilanza.

Quest'ultimo approccio di partnership fra regulated e regulator è suggerito anche da Edwards, che riconosce i limiti di un sistema di compliance basato su regole imposte dall'alto e cerca di incoraggiare lo sviluppo di rapporti fondati sul confronto vicendevole e l'introduzione di elementi di self-regulation, in virtù dei quali indurre gli intermediari ad articolare i propri comportamenti in maniera eticamente corretta, creando rapporti di fiducia reciproca. A questi studi è possibile aggiungere altri due lavori svolti più di recente rispettivamente dalla KPMG e dal Centro Studi Bancari dell'Associazione bancaria Ticinese, che contribuiscono a definire il quadro organizzativo della funzione compliance nel settore finanziario in ambito prevalentemente europeo.

Lo studio proposto dalla KPMG aveva l'obiettivo di raccogliere informazioni sullo stato dell'arte attuale e prospettico della funzioni di compliance dei principali gruppi bancari italiani e internazionali operanti in Italia. La ricerca è stata condotta nel periodo febbraio–marzo 2006 e ha

coinvolto otto banche italiane e sette banche estere. Nonostante il ridotto numero di intermediari coinvolti nell'indagine, il lavoro ha il pregio di fornire elementi utili di natura organizzativa e operativa riguardo all'applicazione della funzione compliance in Italia.

Gli stessi autori, tuttavia, riconoscono come le scelte organizzative operate dalle banche italiane, risultano spesso provvisorie e non esaustive, anche considerato il generale clima di incertezza presente sul mercato domestico. Tutti gli intermediari interpellati dimostrano interesse per le tematiche relative all'attività di compliance e il 50% di essi (non bisogna dimenticare che si tratta dei maggiori gruppi bancari italiani) dispone di una struttura dedicata esclusivamente alla verifica della conformità, contro la totalità (100%) degli intermediari esteri, mentre nel 33% dei casi esiste un sistema strutturato di presidi organizzativi coordinati da un responsabile che risponde ai vertici della banca.

L'indagine compiuta in Svizzera da Pizolli, invece, descrive la situazione della realtà bancaria ticinese e il livello di sviluppo dell'attività di compliance e rappresenta un utile termine di raffronto con il contesto italiano. Pizolli ha condotto la sua indagine nel periodo giugno-luglio 2006, attraverso la somministrazione di un questionario a 84 intermediari finanziari, le risposte ricevute sono state 30, pari al 37% degli interpellati. Gli istituti ticinesi, anche quelli di dimensioni più ridotte, risultano conformi alle richieste più importanti in materia di controlli interni. Tutti gli istituti dispongono di una funzione di Compliance, in media già da sei anni, con un raggio d'azione che investe l'intera attività bancaria e "fondata su una concezione in base alla quale il compliance officer non è visto come un controllore/poliziotto ma piuttosto come un consulente al servizio della banca che agisce preventivamente e mira ad anticipare i cambiamenti normativi anziché adattarvisi a posteriori".

Le considerazioni appena esposte sono, al contrario, smentite in una ulteriore indagine compiuta nel 2005 in Australia, su un campione di 999 aziende fra quelle a maggiore capitalizzazione, da Parker e Nielsen. Gli autori dimostrano che i processi di implementazione della compliance avviati nelle aziende australiane sono in prevalenza parziali e meramente simbolici; essi non sposerebbero, pertanto, lo spirito della compliance, ma sarebbero piuttosto indotti dalla volontà di minimizzare i costi derivanti da multe o sanzioni impartite dalle autorità di mercato.

2.4 La definizione e la quantificazione dei costi di compliance

L'analisi dei contributi presenti in letteratura riguardo alla quantificazione dei costi inerenti all'attività di compliance, presenta aspetti più complessi rispetto a quelli incontrati fino ad ora; alcuni degli studi prodotti riguardano i soli costi sostenuti per l'adeguamento a specifiche richieste regolamentari o ad un gruppo di queste, mentre più difficilmente si valutano i costi sostenuti per introdurre ex-novo un processo di verifica e coordinamento dell'intera attività di compliance.

Come noto, i sistemi contabili usati dalle banche non distinguono i costi sopportati per l'attuazione di norme o regolamenti dagli altri costi della gestione aziendale, pertanto le ricerche compiute in questo campo si basano per lo più su indagini campionarie appositamente ideate per raccogliere questo tipo di informazioni, oppure ricorrono all'ausilio di metodi econometrici per la stima dei costi stessi.

L'obiettivo perseguito è quello di valutare il rapporto costi–benefici della regolamentazione; a tal fine è, evidentemente, necessario analizzare e comprendere il processo di adeguamento alle regole, che presenta elementi peculiari in ogni banca, in funzione dei diversi tratti caratteristici: la dimensione, l'appartenenza a gruppi di banche nazionali o internazionali, la

tipologia di attività svolta. Al riguardo, Llewellen afferma che "Public debate is distorted by the almost exclusive emphasis on costs and it leads to simple assertions that the costs of regulation greatly exceed the benefits because the costs are allegedly high" e, per dimostrare ciò, cita gli alti costi potenziali del fallimento dei mercati: and committed trade practices compliance system, one with all the 'bells and whistles'». "If regulation can prevent these failures or mitigate their effects the savings may be large andgreatly exceed the regulatory costs". Ai fini del presente lavoro, ci si limiterà, in ogni caso, a riportare solo alcuni tentativi di classificazione dei costi di regolamentazione che coinvolgono anche la definizione dei costi di compliance.

Lo studio di Franks propone un tentativo di stima dei costi diretti e indiretti della compliance per i maggiori settori del sistema finanziario in Gran Bretagna. Qui, i costi di compliance vengono definiti come la somma degli oneri relativi allo staff dedicato a tempo pieno o parziale all'attività di compliance, quelli sostenuti per la formazione del personale, per le spese legali e l'acquisizione di sistemi informatici per la gestione di tali attività. Mentre i costi incrementali di compliance sono definiti come "the amount by which compliance costs exceed the costs that would be incurred in the course of normal good business practice". La ricerca perviene anche ad una stima per categorie delle principali voci di costo:

Elliehausen distingue i costi della regolamentazione in Opportunity cost e Operating cost; i primi si hanno quando una norma o una nuova regolamentazione impedisce di intraprendere attività profittevoli; mentre i secondi, i costi operativi, si sostengono quando è richiesto di mettere in atto determinate attività o comportamenti; questi ultimi si distinguono ulteriormente in start-up cost e ongoing cost.

Gli start-up cost sono sostenuti una sola volta, all'inizio del processo di conformazione alle nuove disposizioni regolamentari, ed includono le spese legali per interpretare la norma, le consulenze necessarie per rivisitare le procedure interne, le attività utili a coordinare le funzioni di compliance, i costi sostenuti per modificare i sistemi informativi o programmare e testare i software occorrenti. Gli ongoing cost sono, invece, i costi che ricorrono periodicamente perché inerenti le attività richieste dalla regolamentazione; essi includono le spese per il personale impiegato nell'attività di compliance, per la preparazione dei report o della disclosure ai clienti. L'autore stesso riconosce, in ogni modo, che la distinzione fra start-up e ongoing cost non è spesso così netta. Egli, infine, introduce un'altra definizione, distinguendo il costo totale di una regolamentazione dal costo incrementale; come suggerito dagli stessi termini, per costo totale si intende il costo sostenuto per la messa in opera di tutte le attività richieste dalla regolamentazione; mentre il costo incrementale fa riferimento solo a quei costi imputabili esclusivamente alle prescrizioni della singola nuova norma.

In altri termini, mentre i total cost includono anche costi che le banche sosterrebbero in ogni caso, indipendentemente dalle specifiche prescrizioni regolamentari, gli incremental cost vanno a misurare solo gli oneri sostenuti esclusivamente per gli specifici adeguamenti a singole nuove norme: è perciò evidente che i costi incrementali sono più adatti a rappresentare il costo economico effettivo della regolamentazione.

Secondo Alfon e Andrews i costi della regolamentazione finanziaria possono essere classificati in tre categorie: direct costs, compliance costs, indirect costs.

I direct cost sono tutti quei costi legati a "the value of extra resources that would be absorbed by the regulatory regime in respect of a proposal", durante le fasi di "designing, monitoring and enforcing regulations".

I compliance cost possono essere definiti, invece, come “the value of extra resources (including time) that would be used by firms and/or individuals to comply with a regulatory proposal”.

Gli Autori distinguono, pertanto, la fase di definizione, studio e valutazione di una norma, attuata dall’autorità di vigilanza, dalla fase di adeguamento alla norma stessa da parte delle imprese e fanno sempre riferimento alle cosiddette extra resource, vale a dire ai costi incrementali che la regolamentazione comporta rispetto allo stato di assenza delle regole.

Essi asseriscono che, in una visione estrema, tutti i costi potrebbero essere considerati incrementali (i costi che si sosterrebbero a causa dell’assenza di una regolamentazione, in tal caso, sarebbero ritenuti nulli); tuttavia le diffuse asimmetrie informative, alla base della teoria dei Lemons di Akerlof, dimostrano che un mercato privo di regole può condurre al fallimento e, pertanto, essendo i costi connessi alla mancanza di una regolamentazione adeguata certamente maggiori di zero, ha senso parlare di costi incrementali.

L’ultima classificazione proposta da Alfon e Andrews definisce i costi indiretti di una regolamentazione come i “negative market impacts”. Tali costi sono senza dubbio quelli più difficili da quantificare, perché incerti sia nell’ammontare che nella probabilità di verificarsi; pertanto non possono essere identificati attraverso una cash perspective. Essi includono, fra gli altri, i costi dovuti ad una riduzione della concorrenza e all’imposizione di uniformità fra le imprese, che limitano i vantaggi competitivi.

Una misura regolamentare, dunque, sarà efficace solo quando i suoi benefici economici eccederanno i relativi costi economici in misura superiore alla somma dei costi diretti e dei costi di compliance.

Un ulteriore tentativo di classificazione è stato proposto con uno studio di Fernandez, che raggruppa i costi diretti e indiretti della compliance in quattro categorie: staff-related; outof-pocket; capital; opportunity cost.

I costi relativi al personale impiegato nell'attività di compliance (staff-related) sono generalmente considerati quelli più facilmente quantificabili, perché riconducibili ai salari pagati al personale a vario titolo coinvolto nell'attività in oggetto. Per definire correttamente l'ammontare di questi costi, tuttavia, deve essere tenuta in conto sia la quota dell'orario di lavoro dedicata al perseguimento degli obiettivi di conformità, sia gli eventuali benefit pagati a tale titolo. Questa valutazione è ritenuta più efficacemente praticabile qualora oggetto di valutazione siano le frazioni di tempo riferite a interi dipartimenti, a cui poi verrebbe applicata la media generale dei salari percepiti; la sommatoria dei costi del personale, per ogni dipartimento, fornirebbe la misura degli staff-related cost.

Oltre ai costi del personale dipendente, devono essere considerati, inoltre, quelli relativi al reperimento di alcuni servizi in out-sourcing, per la fornitura di consulenze o professionalità ricollegabili all'attività di compliance; tali costi sono quelli definiti da Fernandez "out-of-pocket".

Con il termine capital-cost si fa, invece, riferimento agli investimenti di capitale riconducibili alla funzione compliance, come l'acquisizione di software specifici, o di apparecchiature e strutture idonee al perseguimento degli obiettivi prefissati. L'ultima classificazione prevede i "costi opportunità", che vengono calcolati in relazione al personale solo parzialmente impiegato nelle funzioni svolte dalla compliance: il tempo dedicato ai nuovi obiettivi è sottratto allo svolgimento di attività che in precedenza svolgeva a tempo pieno, pertanto, è possibile che si generino minori guadagni dallo svolgimento dell'attività precedente, la riduzione di questi guadagni può essere considerata come un costo opportunità. Il

differenziale fra la percentuale di tempo dedicata dal personale impiegato a tempo parziale nell'attività di compliance, prima e dopo l'introduzione della nuova funzione, può fornire un'idea del costo opportunità potenzialmente sopportabile, ma è evidentemente di non facile quantificazione.

L'indagine effettuata dalla società di consulenza Europe Economics per conto della FSA (Financial Services Authority britannica) nel giugno del 2003, riguardo al livello dei costi di compliance sopportati dagli intermediari finanziari chiamati alla conformità ai regolamenti emanati dall'Autorità, ha rivelato quale sia la percezione delle imprese riguardo ai metodi più efficaci per minimizzare i costi di compliance; vengono indicati in ordine di importanza, il sostegno da parte del senior management; la capacità di evidenziare il legame esistente fra una diffusa cultura della compliance e i benefici commerciali che ne derivano, ad iniziare dalla tutela del brand; il garantire una posizione di prossimità e visibilità rispetto al business della funzione compliance; l'istituire un efficiente sistema di monitoraggio periodico dei rischi, anche attraverso l'uso di strumentazione elettronica; gestire in maniera efficace le relazioni con l'autorità di vigilanza, al fine di garantire uno scambio costante di opinioni e una cooperazione duratura.

Al contrario, l'indagine non trova elementi di correlazione fra l'efficienza della funzione compliance ed una serie di altri fattori fra i quali: la dimensione dello staff, l'integrazione dell'attività di compliance all'interno della funzione di risk management, la presenza di un responsabile della compliance all'interno del consiglio di amministrazione, il ricorso a consulenti esterni.

2.5 Il profilo tipico del Compliance officer

Weber e Fortun hanno delineato le caratteristiche tipiche dell'Ethics Compliance Officer a partire da una indagine campionaria che ha coinvolto ventotto imprese. La figura che i due autori descrivono è quella di un maschio di 48 anni circa, che lavora in azienda in media da quattordici anni e che riveste la posizione di responsabile dei programmi etici e di compliance per almeno tre anni. Il titolo attribuito a questo soggetto è difficilmente individuabile in maniera univoca, poiché si è rilevata una grande varietà di appellativi a seconda delle aziende, tuttavia, con buone probabilità, il titolo di riferimento contiene la parola "compliance", e il compliance officer ha una posizione di livello dirigenziale.

Il bagaglio culturale prevede, normalmente, o una laurea in legge o in economia e le funzioni principali che riveste sono quelle di: assicurare la supervisione del programma di compliance; compiere indagini per verificare la presenza di eventuali comportamenti illeciti; eseguire i programmi di aggiornamento e formazione del personale.

Il compliance officer riferisce dell'attività di compliance al consiglio di amministrazione o comunque ai più alti livelli dell'esecutivo. La funzione di compliance è dotata di uno staff con un numero medio di impiegati inferiore a cinque. Weber e Fortun individuano, infine, alcune raccomandazioni, fra le quali quella di prevedere per il compliance officer una posizione autorevole (as a board-level employee) con l'obbligo di un report periodico direttamente ai membri del Consiglio di Amministrazione, al fine di consentire loro di avere un aggiornamento costante, puntuale e senza filtri alle informazioni critiche che riguardano la sfera dei principi etici e di compliance.

La seconda raccomandazione, di importanza forse anche maggiore se applicata al contesto italiano, consiste nel garantire che, con l'aumento delle competenze e delle responsabilità dell'Ethics Compliance Office, si provveda ad incrementare anche le risorse, umane ed economiche, assegnate alla funzione. Infine, anche in questo caso, si ritiene che sia fondamentale la presenza di un forte commitment da parte del senior management. L'indagine, compiuta nell'estate del 2004, ha come campione di riferimento 28 aziende appartenenti all'Associazione Pittsburgh Ethics Network, il tasso di risposta è stato del 50% (14 aziende). I settori economici di appartenenza sono quello finanziario, il settore manifatturiero e sanitario.

2.6 La funzione compliance secondo l'approccio di Basilea

Anche in ambito internazionale sono state avanzate ipotesi in relazione alla gestione del rischio di compliance in banca, in particolare il Comitato di Basilea ha recentemente pubblicato un documento titolato "Compliance and compliance function in banks", a seguito di un periodo di consultazione protrattosi dall'ottobre 2003 al gennaio del 2004. Con questo documento il Comitato si propone di fornire un indirizzo alle banche nella gestione dei rischi di compliance che esso stesso definisce come "risk of legal or regulatory sanctions, material financial loss, or loss to reputation a bank may suffer as a result of its failure to comply with laws, regulations, rules, related self-regulatory organisation standards, and codes of conduct applicable to its banking activities".

Il documento prende in considerazione la costituzione di un'unità di compliance in ogni banca con lo scopo di identificare, valutare, gestire e monitorare il rischio di compliance. L'attività consiste, pertanto, nell'analisi

dell'esistenza di gap fra i vincoli normativi o regolamentari e il sistema di regole interno alla banca e nella predisposizione di una serie di azioni di carattere propositivo e consultivo finalizzate all'annullamento di tali gap e al controllo del rischio che ne deriverebbe.

L'ambito normativo oggetto della funzione compliance appare ampio, comprendendo sia norme di impatto generale, sia regolamenti, standard e codici di condotta interni; le linee guida contenute nel documento dovranno essere adattate di volta in volta allo specifico contesto regolamentare ed economico in cui i singoli intermediari si trovano ad operare, alla struttura e alle dimensioni proprie, nonché alla natura dell'attività svolta.

Le banche possono decidere di inserire la funzione compliance nell'ambito dell'unità di operational risk management, in considerazione dello stretto legame esistente fra le due attività, oppure stabilire un'unità di compliance separata da quella di gestione dei rischi operativi, prevedendo comunque una interconnessione tra esse. Indipendentemente dall'organizzazione interna alla banca il Comitato richiede che la funzione sia dotata di sufficienti risorse finanziarie per compiere la sua attività di verifica e prevenzione, che sia chiaramente esplicitata l'attribuzione delle responsabilità e che l'attività sia regolarmente sottoposta alla supervisione della funzione di Revisione Interna.

Inoltre, il Comitato, consapevole della difficoltà per alcune banche di applicare tutte le specifiche misure contenute nel documento, prevede la possibilità di utilizzare regole diverse, purché tese al raggiungimento dei medesimi risultati.

Il contributo in termini di novità del documento è rappresentato "dalla necessità di una trasversalità dell'azione di presidio coordinata da un'apposita funzione", si tratta infatti di una funzione che coinvolge l'intera sfera dell'attività bancaria. La prima parte del documento, la cui versione

definitiva è stata resa nota nell'aprile del 2005, descrive (Principles 1, 2, 3, 4) le specifiche responsabilità del board of directors (consiglio di amministrazione) e del senior management; i principi riportati dovrebbero essere applicati in accordo con la struttura di corporate governance di ogni banca, gruppo bancario o holding company, le cui società svolgono prevalentemente attività bancaria.

Il primo principio è dedicato alle responsabilità di supervisione del rischio di compliance da parte del consiglio di amministrazione; il Comitato stabilisce che esso deve approvare la compliance policy della banca, descritta in un apposito documento e, almeno una volta all'anno, il consiglio di amministrazione, o una commissione interna (the board or a committee of the board) a cui sia stato appositamente delegato questo compito, dovrà valutare la qualità della gestione del rischio di compliance; a tal fine il consiglio di amministrazione riceve periodicamente dai senior manager un rapporto dell'attività di gestione del rischio. I principi seguenti, dal secondo al quarto, riguardano le responsabilità del senior management, che è considerato il centro responsabile della efficiente gestione del rischio di compliance; esso deve formulare per iscritto e rendere nota una politica di gestione della compliance e, almeno una volta all'anno, deve effettuare il reporting al consiglio di amministrazione della gestione del rischio; altre comunicazioni possono essere comunque intraprese, aldilà della ordinaria reportistica, quando sia necessario.

La compliance policy deve contenere i principi di base che devono essere seguiti e descrivere i principali processi attraverso i quali i rischi di compliance possono essere identificati e i piani attraverso i quali possono essere gestiti nei diversi livelli dell'organizzazione aziendale.

In particolare dovranno essere indicati in maniera chiara e trasparente gli standard di carattere generale applicabili a tutti i membri dello staff e i ruoli

attribuiti a specifici gruppi del personale; inoltre, dovrà essere indicata la relazione esistente con le altre funzioni di risk management e con la funzione di revisione interna.

Il senior management deve assicurarsi che la politica di compliance sia osservata e qualora si ravvisino violazioni è responsabile di approntare gli appropriati rimedi o azioni disciplinari. Infine, i senior manager sono incaricati di assicurare alla banca una funzione compliance permanente ed efficace in base ai criteri dettati dal Comitato di Basilea e descritti nei seguenti principi dal 5 all'8. Il primo criterio (principle 5) stabilisce che: "The bank's compliance function should be independent"; da questa affermazione discende che:

- la funzione compliance dovrebbe avere uno status formale, tale da attribuire alla stessa una posizione adeguata all'interno della banca, una appropriata autorità e la giusta indipendenza;
- dovrebbe essere individuato un head of compliance responsabile della gestione del rischio di compliance;
- l'intero staff che si occupa della gestione del rischio di compliance deve essere messo nella condizione di non trovarsi a gestire possibili conflitti d'interesse fra la specifica responsabilità derivante dal proprio ufficio e qualsiasi altra possa derivare da attività alternative o complementari;
- lo staff che si occupa della funzione compliance deve poter accedere a tutte le informazioni necessarie allo svolgimento della propria attività, richiedere l'assistenza di specialisti interni o esterni alla banca, effettuare investigazioni.

Il Comitato di Basilea specifica che l'indipendenza sancita dal principle 5 non deve essere intesa come una impossibilità di lavorare a stretto contatto

con le altre funzioni aziendali; la cooperazione è invece auspicabile se può aiutare a identificare e gestire i rischi di compliance in uno stadio iniziale.

La separazione fra l'attività di compliance e le responsabilità derivanti dallo svolgimento di qualsiasi altra attività all'interno della banca può essere difficile da realizzare in caso di banche di piccole dimensioni o in filiali; in questi casi deve comunque essere evitato il potenziale conflitto d'interesse.

Il documento prende in considerazione anche i conflitti generati dai meccanismi di remunerazione del personale collegati alle performance finanziarie delle linee di business per le quali essi esercitano la loro attività di compliance, in tal caso il Comitato asserisce che questa tipologia di remunerazione può essere generalmente accettata, ma deve essere tenuto sotto controllo il possibile conflitto che ne deriva.

Il secondo criterio (principle 6) prevede che la funzione compliance sia dotata di congrue risorse umane e materiali per tendere efficacemente agli obiettivi ad essa affidati.Il personale coinvolto nell'attività di compliance (compliance staff) deve possedere appropriate qualità personali e professionali, inclusa la padronanza di leggi, regolamenti, standard e del loro pratico impatto sulla operatività delle banche; tali competenze devono fra l'altro essere costantemente aggiornate ed approfondite prevedendo periodici momenti di studio. Il principle 7 definisce la responsabilità della funzione compliance nella banca, che consiste nell'assistere il senior management nella efficiente gestione del rischio fronteggiato dalla banca. Questa responsabilità può essere esercitata all'interno di un'unica compliance unit, oppure in diversi dipartimenti: ci sono casi in cui la funzione in questione può essere svolta all'interno del gruppo che si occupa dell'operational risk management; casi in cui la fase di advising management è affrontata da un dipartimento (ufficio legale), mentre l'unità

di compliance è dedicata al monitoraggio e al reporting all'organo di amministrazione.

L'eventuale divisione delle responsabilità fra più dipartimenti della banca deve però essere chiara e devono essere previsti altrettanto chiari legami di cooperazione fra di essi, in un meccanismo che garantisca la gestione efficiente dei rischi.

La funzione compliance inoltre:

- deve consigliare il senior management sulla conformità a leggi, regolamenti e standard, e tenerlo informato sugli sviluppi relativi;
- deve assistere il senior management nella formazione e aggiornamento dello staff e nel predisporre una guida scritta per la verifica di coerenza della
- conformità alle normative, attraverso politiche, procedure codici di condotta interna e quant'altro ritenuto necessario;
- deve identificare, misurare e gestire in maniera propositiva i rischi di compliance in banca;
- deve monitorare ed esaminare la compliance attraverso la predisposizione di adeguati test, i cui risultati dovranno essere comunicati all'organo amministrativo;
- può avere specifiche responsabilità legali (per esempio antiriciclaggio) in virtù delle quali può istituire specifiche relazioni con organi esterni alla banca;
- deve redigere un compliance programme in cui sono riportate le responsabilità, le politiche, le procedure, i test di valutazione del rischio, i programmi di formazione e aggiornamento dello staff a cui si è fatto riferimento nei punti precedenti.

Con riferimento ai rapporti della funzione compliance con altri organi aziendali, il Comitato di Basilea indica, al principle 8, che gli ambiti di

applicazione dell'attività di compliance sono sottoposti a periodiche revisioni dalla funzione di internal audit; specificando in seguito che questo implica una separazione fra la funzione di internal audit e la funzione compliance, al fine di assicurare che quest'ultima sia assoggettata ad una revisione indipendente, e che esista un chiaro accordo scritto riguardo alla suddivisione delle attività di gestione dei rischi e di testing fra le due unità. Tale disposizione assume un'importanza crescente alla luce dei dati rilevati dall'analisi empirica, di seguito presentati, dai quali si evince che, soprattutto nelle banche di dimensione minore, la distinzione fra attività di compliance e altre funzioni aziendali, prima fra tutte quelle relative ai controlli interni dell'Auditing, non è così netta. Gli ultimi due principi riportati nel documento "Compliance and compliance function in banks" sono classificati sotto la voce "Other matters".

Il numero 9 stabilisce che la banca deve garantire la compliance con le leggi, i regolamenti e gli standard di tutti i sistemi legislativi in cui svolge la sua attività di business.

Infine, il principio numero 10, ricordando che specifici compiti della funzione compliance possono essere esternalizzati, stabilisce che, in ogni caso, questi devono essere assoggettati alla necessaria supervisione da parte del compliance officer e che il consiglio di amministrazione e il senior management restano responsabili della conformità al sistema di norme e regolamenti in cui opera la banca.

2.7 Materie rilevanti ai fini della compliance: D.lgs. n. 231/2001

Con il D.lgs. n. 231/2001 è stato introdotto nell'ordinamento italiano un complesso e innovativo sistema sanzionatorio che prefigura forme di responsabilità amministrativa a carico degli enti (sia enti forniti di

personalità giuridica, sia le società e associazioni anche prive di personalità giuridica) per reati commessi nel loro interesse o a loro vantaggio da soggetti che rivestono una posizione di rilievo nella struttura dell'ente medesimo, ovvero da soggetti sottoposti alla vigilanza di questi ultimi.

Tale responsabilità si aggiunge a quella della persona fisica che ha materialmente realizzato il fatto e sussiste anche quando l'autore del reato non è stato identificato, il reato si estingue per causa diversa dall'amnistia e sia stato commesso all'estero da enti aventi la loro sede principale nel territorio nazionale, purché per lo stesso non proceda lo Stato presso cui è stato commesso il reato.

Affinché l'ente sia ritenuto responsabile occorre che il reato sia riconducibile all'ente e che sussista la sua colpevolezza.

Il sistema delineato dal D.lgs. n. 231/2001 ed il "sistema Compliance" presentano, dal punto di vista sistematico, molti profili di contatto – tali da creare forme di collaborazione tra la Funzione di Compliance e l'organo di vigilanza di cui al D.lgs. n. 231/2001 - ma anche numerose differenze.

Il Decreto n. 231/2001, nell'introdurre nell'ordinamento un nuovo tipo di responsabilità amministrativa a carico degli enti connessa ad un fatto di reato posto in essere da vertici o dipendenti dell'ente stesso, ha anche previsto criteri di possibile esenzione da tale responsabilità. L' eventuale esenzione da tale responsabilità passa attraverso la verifica, da parte del giudice penale, che l'ente abbia adottato ed efficacemente attuato "modelli organizzativi" idonei alla prevenzione del reato verificatosi. Il giudice penale dovrà verificare la sussistenza o meno in capo all'ente di una cosiddetta colpa organizzativa.

I principali punti di contatto tra Compliance e 231 sono:

- entrambe le discipline attribuiscono “rilevanza” all’organizzazione dell’ente ed al connesso sistema di prevenzione del rischio;
- entrambe postulano la costruzione di un modello aziendale che segue gli stessi passaggi logici (mappatura del rischio, verifica di congruità delle procedure esistenti ecc.);
- entrambe le discipline lasciano ampio margine di autonomia nelle modalità concrete di costruzione di tale modello di prevenzione;
- in entrambe le discipline responsabile della costruzione del sistema di prevenzione è l’organo con funzioni gestorie;
- entrambe prevedono la creazione di un soggetto che vigila sul modello di prevenzione, con caratteristiche simili (autonomia, indipendenza ecc);
- entrambe agiscono ex ante e non entrano nel merito dei comportamenti dei singoli.

Sono tuttavia rilevanti anche le differenze:

- Il D.lgs. n. 231/2001 si riferisce non solo alle Banche, ma anche a tutti gli enti;
- Il “sistema 231” è meramente opzionale;
- Il D.lgs. n. 231/2001 ha un “perimetro” che è indicato dalla stessa legge;
- L’Organismo di Vigilanza 231 non fa parte del sistema di controllo interno; tra Compliance e Organismo di Vigilanza vi sono sinergie e coordinamenti, ma i due soggetti non possono essere accomunati;
- Il rischio che entrambi i sistemi prevengono è solo in parte coincidente: il rischio 231 è solo rischio di sanzione, anche se tale modello deve funzionare a prescindere dalla rilevanza penale delle violazioni.

Concludendo, Compliance e Organismo di vigilanza ai sensi del Decreto 231/2001 sono due esempi di un approccio legislativo comune che trasla sul vigilato l'onere di regolazione.

Un approccio sinergico alla prevenzione dei rischi impone alla Banca di prefigurare forme di collaborazione tra i soggetti Compliance e soggetti 231.

2.8 Materie rilevanti ai fini della compliance: Legge MIFID

Markets in Financial Instruments Directive, è la direttiva 2004/39/CE del Parlamento Europeo e del Consiglio del 21 aprile 2004, che costituisce un passo importante verso la costruzione di un mercato finanziario integrato efficace e competitivo all'interno dell'Unione Europea (UE).

La direttiva si inquadra nel più ampio *Piano di Azione per i Servizi Finanziari* (FSAP); ed è entrata in vigore nel 2007.

La direttiva in questione è applicabile a tutte le imprese di investimento, compresi gli enti creditizi, ed ha come scopo principale quello di regolamentare l'esecuzione di alcuni servizi o attività di investimento, compresi tutti quelli inerenti agli strumenti finanziari.

La MiFID introduce anche un più ricco elenco di strumenti finanziari, tra cui valori mobiliari, strumenti di mercato monetario, quote di organismi di investimento collettivo, derivati, opzioni, indici, valute, *future*, *swap*, contratti finanziari con trasferimento di rischio di credito, contratti finanziari differenziali, contratti su variazioni climatiche e molti altri.

La direttiva abolisce l'obbligo di concentrazione nei mercati regolamentati, ed introduce nuove forme di scambio, quali i sistemi multilaterali di negoziazione (MTF).

A fronte di una possibile pluralità di luoghi in cui gli strumenti finanziari sono negoziati, la direttiva ridisegna gli obblighi di esecuzione degli ordini dei clienti alle migliori condizioni (c.d. *best execution*), prevedendo che gli intermediari stabiliscano una propria *execution policy* ("politica di esecuzione"), nella quale indicare, per ciascuna tipologia di strumento, le sedi di esecuzione su cui verranno eseguiti gli ordini di compravendita e i fattori di esecuzione che verranno considerati per la scelta della sede che fornisce il miglior risultato possibile.

Le funzioni di controllo sono demandate alla Funzione di Compliance con il compito di verificare il rispetto della normativa.

Le autorità e gli intermediari dovranno adottare ogni misura ragionevole per identificare i conflitti d'interesse che possono nuocere ai clienti, e di renderli maggiormente visibili.

La MIFID ha tra i suoi obiettivi principali quello di creare un ambiente finanziario competitivo e armonizzato per i mercati regolamentati e le imprese di investimento, nonché quello di rafforzare la protezione degli investitori, l'efficienza e l'integrità dei mercati finanziari stessi.

Più in particolare, la MIFID introduce delle novità sia nei confronti degli intermediari che dei mercati.

Le principali norme relative agli intermediari riguardano:

- i requisiti di organizzazione nonché l'esternalizzazione delle funzioni operative;
- i conflitti di interessi e le relative politiche di gestione degli stessi;
- le ricerche in materia di investimenti;

- la disciplina degli incentivi nonché le informazioni fornite ai clienti;
- le registrazioni degli ordini e delle operazioni eseguite;
- le informazioni fornite ai clienti e potenziali clienti;
- la classificazione della clientela in *retail*, *professional*, *eligible counterparties*;
- le valutazioni di adeguatezza e appropriatezza dei servizi di investimento prestati ai clienti;
- la gestione degli ordini dei clienti (*client order handling rules*);
- la consulenza in materia di investimenti;
- la disciplina della *best execution* al fine di assicurare la migliore esecuzione degli ordini ai clienti;
- le nuove categorie dei servizi di investimento.

Al contrario, le principali norme relative ai mercati sono rappresentate da:

- l'eliminazione dell'obbligo di concentrare gli scambi sui mercati regolamentati;
- le nuove figure di *trading venues*, rappresentate dai mercati regolamentati, i *multilateral trading facilities* (MTF) e gli internalizzatori;
- le regole di trasparenza *pre-trade* e *post-trade* delle informazioni di mercato;
- specifiche previsioni per l'ammissione degli strumenti finanziari sui mercati regolamentati;
- le regole per l'ammissione degli operatori ai mercati regolamentati ed agli MTF.

Le regole di Basilea II prevedono, accanto ai requisiti patrimoniali minimi proporzionali ai rischi, un "secondo pilastro" costituito dall'obbligo per l'intermediario di valutare l'esistenza di altri rischi non presi in considerazione nei requisiti minimi, l'adeguatezza dell'apparato dei

controlli nel fronteggiare tutti i rischi, l'eventuale necessità di mantenere un capitale superiore ai minimi per coprire il "rischio residuale".

Più specificamente rivolte ai rischi legali e di reputazione sono le regole che richiedono la costituzione, nell'ambito del sistema dei controlli interni, della Funzione di *Compliance*, incaricata di verificare che in tutti i settori operativi della Banca esistano meccanismi che assicurino il rispetto delle norme applicabili all'attività bancaria, e in particolare di quelle che si riferiscono ai rapporti con la clientela e alla tutela del consumatore.

L'aspettativa che la disciplina della funzione di conformità alle norme riduca i rischi legali e di reputazione è rafforzata dall' attuazione della direttiva MiFID.

La direttiva non solo introduce una più chiara articolazione delle tutele da fornire a ciascuna categoria di clientela per i diversi tipi di servizi forniti, ma fa anche ricorso alla tecnica regolamentare di individuare gli obiettivi di tutela che gli intermediari devono perseguire, lasciando ad essi l'individuazione delle soluzioni organizzative e alle autorità di controllo il compito di valutarne l'adeguatezza. Questa tecnica è potenzialmente in grado di ottenere il miglior equilibrio fra la protezione degli utenti e il contenimento dei costi e, soprattutto, delle incertezze per gli intermediari.

In effetti la riduzione dell'incertezza - su diritti e doveri, sui comportamenti richiesti a ciascuno - facilita il raggiungimento di entrambi gli obiettivi della tutela dei risparmiatori e del contenimento dei rischi degli intermediari.

Nella definizione della Funzione di Conformità alle norme si realizza un primo test della possibilità di perseguire i due distinti obiettivi di tutela dei risparmiatori e di contenimento dei rischi degli intermediari senza creare tensioni sul piano applicativo.

I requisiti richiesti per la funzione nella regolamentazione prudenziale delle Banche e nella MiFID presentano numerosi aspetti di omogeneità e limitate differenze.

Entrambe le discipline richiedono l'attivazione di una funzione dedicata e permanente. Entrambe indicano l'indipendenza e la qualificazione come requisiti irrinunciabili e individuano uguali presupposti di tali requisiti: l'autonomia del responsabile dalle strutture operative e il riporto diretto agli organi aziendali; risorse e competenze adeguate; la necessità di segregare le attività di controllo della conformità e le attività operative soggette a tali controlli; la separatezza organizzativa dalle altre funzioni di controllo.

Sia la disciplina prudenziale sia la MiFID richiedono che l'attuazione delle norme sulla Funzione di Compliance sia informata al principio di proporzionalità, secondo cui la complessità delle soluzioni organizzative deve riflettere dimensioni e tipo di attività dell'intermediario. La derogabilità al requisito di separatezza organizzativa tra funzioni di controllo è però applicata in maniera diversa: nella disciplina bancaria ha centralità la funzione di gestione dei rischi, in cui può essere allocata anche la funzione di Compliance; la disciplina sui servizi di investimento richiede che sia sempre presente la funzione di conformità, potendosi derogare alla presenza di altre funzioni di controllo indipendenti.

Diverso è, naturalmente, il perimetro di riferimento della Compliance. Nella disciplina della MiFID, esso è limitato alle norme rilevanti per lo svolgimento dei servizi e delle attività di investimento. Nella disciplina prudenziale, il perimetro di riferimento è più ampio; esso comprende, oltre alle regole relative alla prestazione dei servizi di investimento, anche le norme sullo svolgimento delle operazioni e dei servizi bancari e di pagamento, la disciplina di vigilanza prudenziale, l'azione di prevenzione e contrasto del riciclaggio e dell'usura.

Nel complesso, la regolamentazione prudenziale sulla Funzione di Compliance nelle Banche appare pienamente compatibile con quella volta ad assicurare la correttezza e la trasparenza dei comportamenti nella prestazione dei servizi di investimento agli investitori e al mercato.

Conseguentemente, non sembrano esserci ostacoli a che i profili di conformità afferenti a entrambi gli ambiti regolamentari siano gestiti dalla stessa funzione. L'omogeneità sostanziale delle due discipline eviterà di appesantire gli oneri di adeguamento nelle Banche che svolgono servizi di investimento, contribuendo all'efficacia complessiva dei presidi di Compliance.

2.9 Materie rilevanti ai fini della compliance: MAD – Market Abuse Directive

Le gravi crisi societarie e i problemi emersi nel rapporto tra mercato e investitori, che si sono verificati negli ultimi anni in Italia come in altri importanti paesi, hanno segnato profondamente il quadro di riferimento all'interno del quale le autorità di vigilanza svolgono la loro funzione di tutela del risparmio. Sono emerse nuove criticità nell'ambito dei sistemi di governo societario, nelle funzioni di controllo, nei rapporti tra intermediari e investitori, nella crescente globalizzazione delle attività delle imprese e della prestazione dei servizi di investimento.

Dalla manifestazione di tali patologie è derivata una crescente domanda di tutela e una diffusa esigenza di ridefinire obiettivi e priorità dell'attività di vigilanza.

La natura globale di gran parte delle problematiche che si sono manifestate con le crisi ha, d'altra parte, fatto emergere una maggiore consapevolezza dell'esigenza di coordinamento internazionale. I problemi emersi sono

infatti sempre meno affrontabili nell'ambito di regole e strumenti di enforcement di matrice nazionale e l'accresciuta interdipendenza dei mercati aumenta il rischio di trasmissione dei fenomeni di instabilità. Le iniziative di coordinamento e di cooperazione internazionale si sono infatti notevolmente rafforzate, sia su scala "regionale" che globale, con la finalità di definire standard comuni per l'evoluzione della regolamentazione e della vigilanza sui mercati e di salvaguardare la stabilità finanziaria dell'economia mondiale.

Le disposizioni legislative sul Market Abuse sono state introdotte dall'art. 9 della Legge n.62/2005 "Disposizioni per l'adempimento di obblighi derivanti dall'appartenenza dell'Italia alle Comunità europee, Legge comunitaria 2004", che recepisce la Direttiva 2003/6/CE relativa al tema degli Abusi di Mercato.

In relazione a tali previsioni la Consob ha opportunamente aggiornato i Regolamenti Emittenti e Mercati.

Le norme di legge e regolamentari mirano a contrastare gli Abusi di Mercato che ledono l'integrità dei mercati finanziari e compromettono la fiducia degli investitori nei valori mobiliari e negli strumenti derivati, adottando specifiche misure finalizzate a scoraggiare la manipolazione di mercato e l'abuso di informazioni privilegiate ed a favorire una maggiore responsabilità degli operatori. L'attività di prevenzione degli abusi riguarda sia gli emittenti quotati ed i soggetti ad essi collegati, sia gli intermediari abilitati e le società di gestione del mercato.

Per gli intermediari abilitati e le società di gestione del mercato le misure definiscono gli standard di qualità dei comportamenti, con particolare riguardo alla loro correttezza e trasparenza e prevedono criteri per l'identificazione di pratiche di manipolazione, procedure per il

riconoscimento di prassi di mercato ammesse, nonché obblighi di segnalazione all'autorità competente delle operazioni sospette.

Le norme sul Market Abuse, di cui al citato art. 9 della Legge 62/2005 trattano, nello specifico, i seguenti ambiti:

- "Internal Dealing": obbligo di comunicazione al pubblico ed alla Consob delle operazioni effettuate dai soggetti rilevanti, anche per interposta persona, aventi ad oggetto azioni dell'emittente quotato o altri strumenti finanziari ad esse collegate;
- "Acquisto di azioni proprie": definizione delle modalità di acquisto delle azioni e obbligo di comunicazione del programma al mercato;
- "Raccomandazioni": regolamentazione sulla correttezza e trasparenza degli studi e delle ricerche aventi ad oggetto strumenti finanziari quotati;
- "Informazioni privilegiate": introduzione della nozione quale oggetto di disclosure e dell'obbligo di istituzione del "Registro delle persone che hanno accesso a informazioni privilegiate";
- "Registro delle persone che hanno accesso ad informazioni privilegiate": obbligo per gli emittenti ed i soggetti in rapporto di controllo con essi di istituire e gestire il registro delle persone che in virtù dell'attività lavorativa hanno accesso a informazioni privilegiate;
- "Abuso di informazioni privilegiate e manipolazione del mercato".

2.10 Materie rilevanti ai fini della compliance: Antiriciclaggio

L'immissione nel sistema legale delle risorse finanziarie generate dall'usura costituisce, come per le altre attività criminali, un momento di vulnerabilità

per le organizzazioni illegali, in quanto il contatto con operatori economici sani eleva la possibilità di individuare fenomeni illeciti.

Emerge quindi l'importanza della regolamentazione in materia di prevenzione dall'utilizzo del sistema finanziario a scopi di riciclaggio. Essa poggia sui limiti all'uso del contante e degli strumenti di pagamento anonimi, sulla identificazione della clientela e la registrazione dei dati, sulla segnalazione delle operazioni sospette. Per facilitare l'individuazione delle operazioni anomale la Banca d'Italia ha emanato, nel corso degli anni, regole operative volte a ridurre i margini di incertezza connessi con valutazioni soggettive o con comportamenti discrezionali.

Le "istruzioni operative" indicano specifici canoni operativi, incentrano l'attenzione sul profilo della conoscenza della clientela, attribuiscono rilievo al sistema dei controlli interni, definiscono una procedura di segnalazione improntata a celerità e riservatezza.

Al fine di recidere ogni possibile legame tra organizzazioni usurarie e dipendenti infedeli, le "istruzioni" richiamano l'introduzione del reato, previsto appunto dalla legge 108/96, che punisce il dipendente di Banche o di intermediari finanziari che indirizza una persona, per operazioni bancarie o finanziarie, a un soggetto abusivo.

Tale fattispecie ha colmato una lacuna nell'apparato di prevenzione del fenomeno dell'usura consentendo di colpire comportamenti di sostegno all'attività degli usurai provenienti dall'interno degli operatori legali. La tenuità della pena prevista ha verosimilmente limitato l'applicazione giudiziaria del reato.

La seconda parte delle istruzioni riporta una casistica esemplificativa di indici di anomalia, alcuni dei quali sono finalizzati all'individuazione dei fenomeni dell'usura. Partendo da tali indicatori e dall'analisi delle segnalazioni ricevute, l'UIC (Ufficio Italiano Cambi), sostituito da UIF

(Unità d'Informazione Finanziaria) ha fornito indicazioni operative basate sulle analogie di comportamento rilevate nelle movimentazioni finanziarie sospette di usura.

Nel periodo 2001/2006 l'UIC ha analizzato 1.139 segnalazioni di operazioni sospette riconducibili a ipotesi di usura e 497 segnalazioni relative a ipotesi di abusivo esercizio di attività finanziaria. Le operazioni della specie individuate per il 2006 hanno un valore di oltre 18 milioni di Euro.

La costituzione di una unità specializzata antiriciclaggio presso la Banca d'Italia, in occasione dell'unificazione con l'UIC, costituì l'occasione per un rilancio dell'operatività, in particolare attraverso un arricchimento di carattere finanziario svolto prima dell'avvio delle eventuali indagini giudiziarie, una riduzione dei tempi dell'analisi e un rafforzamento delle capacità operative. Si realizzano sinergie con l'attività di Vigilanza e positivi riflessi in termini di prevenzione della criminalità economica nel sistema finanziario.

Tra il 1991 e il 2008 si sono succedute tre Direttive Comunitarie (I, II, III Direttiva Antiriciclaggio) poi recepite nell'Ordinamento Italiano.

Il provvedimento attuativo di recente approvazione è il D.Lgs. n. 231 del 21 Novembre 2007, ovvero la Terza Direttiva in materia di prevenzione dell'utilizzo del sistema finanziario a scopo di riciclaggio dei proventi di attività criminose e di finanziamento al terrorismo.

Il termine riciclaggio riguarda un'azione di reimmissione di profitti ottenuti con operazioni illecite o illegali all'interno del normale circuito economico.

La condotta di riciclaggio è prevista quale reato nel codice penale: gli articoli 648 bis e ter lo inseriscono fra i "Delitti contro il patrimonio". Tali articoli incriminano chiunque "fuori dai casi del concorso nel reato,

sostituisce o trasferisce denaro, beni, ovvero compie in relazione ad essi operazioni in modo da ostacolare l'identificazione della loro provenienza delittuosa".

Nel D.Lgs. n. 231 del 21 Novembre 2007, art. 2, ai soli fini dell'applicazione delle disposizioni del decreto stesso, le seguenti azioni, se commesse intenzionalmente, costituiscono riciclaggio:

- la conversione o il trasferimento di beni, effettuati essendo a conoscenza che essi provengono da un'attività criminosa o da una partecipazione a tale attività, allo scopo di occultare o dissimulare l'origine illecita dei beni medesimi;
- l'occultamento o la dissimulazione della reale natura o provenienza dei beni o dei diritti sugli stessi, effettuati essendo a conoscenza che tali beni provengo da un'attività criminosa;
- l'acquisto o la detenzione di beni provenienti da attività illecite.
- Il finanziamento al terrorismo riguarda invece "qualsiasi attività diretta alla raccolta, alla provvista, all'intermediazione o all'erogazione di fondi o di risorse economiche, destinati ad essere utilizzati al fine di compiere uno o più delitti con finalità di terrorismo" (art. 1, comma 1, lett. A, del D.Lgs. n.109/2007).

L'obbligo di adeguata verifica della clientela da parte degli intermediari ai sensi dell'art. 15 del D.Lgs. 231/07 scatta quando:

- si instaura un rapporto continuativo;
- si eseguono operazioni occasionali, disposte dai clienti che comportino la trasmissione o la movimentazione di mezzi di pagamento di importi pari o superiori a 15.000 euro;
- vi è sospetto di riciclaggio o di finanziamento al terrorismo;
- vi sono dubbi sulla veridicità o sull'adeguatezza dei dati precedentemente ottenuti ai fini dell'identificazione di un cliente.

Fermo restando quanto disposto dal Codice Civile e da Leggi Speciali, il Collegio Sindacale, il Consiglio di Sorveglianza, il Comitato di Controllo di gestione, l'Organismo di Vigilanza (ex D.Lgs. 231/01) e tutti i soggetti incaricati del controllo di gestione comunque denominati vigilano sull'osservanza delle norme in materia di antiriciclaggio.

Le Autorità di Vigilanza di settore nell'ambito delle rispettive competenze verificano l'adeguatezza degli assetti organizzativi e procedurali e il rispetto degli obblighi previsti dal D.Lgs. 231/01.

L'UIF verifica il rispetto delle Disposizioni in tema di prevenzione a contrasto del riciclaggio o del finanziamento del terrorismo con riguardo alle segnalazioni di operazioni sospette e ai casi di omessa segnalazione.

Le attività di verifica e di attestazione della conformità dell'organizzazione aziendale alla legge, svolte dalla Funzione Compliance, hanno una stretta attinenza con la prevenzione del riciclaggio di denaro proveniente da attività illecite che, in quanto tali, precedono per importanza sia le disposizioni dettate da procedure interne, sia quelle eventualmente previste da codici di autodisciplina. Spetta inoltre alla Funzione Compliance esercitare un presidio adeguato a garantire che gli operatori di filiale abbiano consapevolezza del rischio di coinvolgimento in operazioni di riciclaggio. In tal senso alla struttura della Funzione Compliance è demandato un ruolo di deterrenza dell'attività di riciclaggio, da esercitarsi mediante la supervisione dell'attività degli operatori di filiale.

La Funzione Compliance prevede anche l'attuazione di programmi specifici di addestramento e di formazione del personale, che devono essere attuati con carattere di continuità e sistematicità, pena il mancato raggiungimento di un adeguato livello di conformità alla legge. Obiettivo quest'ultimo che non può essere conseguito a prescindere dalla sensibilizzazione di tutto il personale nei confronti delle problematiche inerenti alla materia.

2.11 Materie rilevanti ai fini della compliance: privacy

Con l'entrata in vigore, dal 1° Gennaio 2004, del nuovo codice in materia di protezione dei dati personali (D.Lgs. n. 196/2003) viene razionalizzata la normativa in materia di privacy. Il nuovo Testo Unico ricompone in modo organico le disposizioni introdotte nel nostro ordinamento con la Legge n. 675/1996 denominata "Tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali". Il D.Lgs. n.196/2003 prevede nuove garanzie per i cittadini, razionalizza le norme esistenti e opera la semplificazione di alcuni adempimenti; in particolare per quanto riguarda la notificazione al Garante per la protezione dei dati personali, attraverso la quale ogni Banca rende noto a quest'ultimo di svolgere un'attività di raccolta e di utilizzazione dei dati personali dei propri clienti.

Di particolare rilievo per le Banche sono le novità introdotte con riguardo ai trattamenti di dati mediante l'ausilio di strumenti elettronici, consentito solo se siano adottate delle misure minime, di seguito alcune di esse:

- autenticazione informatica;
- protezione degli strumenti elettronici e dei dati rispetto a trattamenti illeciti;
- tenuta di un aggiornato documento programmatico sulla sicurezza.

Secondo il Codice Privacy l'interessato del trattamento è la persona fisica, la persona giuridica, l'ente o l'associazione a cui si riferiscono i dati personali che possono essere oggetto di trattamento.

In linea generale gli interessati possono essere ricondotti sostanzialmente alle seguenti categorie di soggetti:

- clienti e utenti

- dipendenti
- soggetti terzi
- esponenti aziendali

L'interessato quel "legittimo proprietario" dei dati, è la figura a cui il Codice Privacy riserva specifici diritti, in particolare l'interessato ha diritto:

- di accesso ai dati personali ovvero di ottenere la conferma dell'esistenza o meno di dati che lo riguardano e quindi di venire a conoscenza della loro origine o delle finalità;
- di ottenere l'aggiornamento, l'integrazione dei dati, nonché la cancellazione o la trasformazione in forma anonima;
- di opporsi, in tutto o in parte, al trattamento dei dati personali che lo riguardano, per motivi legittimi.

A garanzia dei suoi diritti, l'interessato può rivolgersi o al Garante per la protezione dei dati personali, organo collegiale che opera in piena autonomia ed è investito dei poteri necessari a vigilare che il trattamento dei dati personali avvenga nel rispetto della normativa, o all'Autorità Giudiziaria Ordinaria.

La dimensione aziendale e la varietà delle problematiche operative da affrontare sono validi motivi per cui all'interno della propria struttura, una Banca, si avvalga di più Responsabili Interni collocando tali punti di responsabilità nei contesti caratterizzanti dai maggiori volumi trattati.

In base a convenzioni ed accordi o per esigenze di carattere organizzativo, sempre più spesso ci si trova ad operare con soggetti terzi, i quali intervengono nei processi di lavorazione di molteplici e svariati servizi richiesti dagli interessati che non vengono gestiti esclusivamente all'interno della Banca.

La responsabilità del governo operativo e della disciplina relativa agli obblighi in materia di Privacy, in coerenza con quanto stabilito dalla normativa vigente e sulla base dell'assetto organizzativo della Banca, può essere attribuito alla Funzione Compliance.

Quest'ultima ha, in particolare, il compito di:

- analizzare e identificare gli interventi finalizzati all'adeguamento alle norme sulla Privacy;
- applicare le politiche di gestione e rapporto con gli Organi di Vertice;
- svolgere una costante attività di supervisione della conformità dei processi operativi interni alla normativa Privacy.

2.12 Materie rilevanti ai fini della compliance: Antiusura

La fattispecie dell'usura consiste nell'approfittare di una situazione di bisogno finanziario di una persona o di un'impresa per imporre condizioni particolarmente esose sul prestito a essa concesso. L'obiettivo principale di un contratto usuraio è spesso quello di impadronirsi, con modalità illecite, della garanzia del prestito (ad esempio, l'impresa stessa) o comunque di quanto economicamente rilevante può essere sottratto alla vittima.

Presupposto dell'usura è che la vittima non abbia accesso al credito bancario, per motivi oggettivi o soggettivi; sul piano della prevenzione assumono rilievo strategico, quindi, le misure per facilitare l'accesso ai finanziamenti bancari per i soggetti che incontrano difficoltà e per fornire alle famiglie e alle piccole imprese una conoscenza finanziaria adeguata rispetto alle loro esigenze. Resta fermo che compito delle Banche è evitare

che, in assenza di prospettive, i clienti accrescano il proprio livello di indebitamento, aggravando in tal modo la loro situazione personale.

All'azione di prevenzione del fenomeno dell'usura contribuisce l'attività di controllo esercitata dalle autorità amministrative al fine di evitare il coinvolgimento del sistema finanziario. Nella regolamentazione delle Banche e degli intermediari è chiara la consapevolezza di dover porre alla base del funzionamento dei mercati l'integrità e cioè il rispetto delle regole non solo tecniche, ma anche etiche e giuridiche.

Il primo presidio posto a tutela dell'integrità del sistema finanziario consiste nel contrasto alle forme di abusivismo bancario e finanziario, che presentano evidenti connessioni con il reato di usura. Al di fuori della legalità si collocano talvolta società finanziarie di modeste dimensioni, non iscritte nell'elenco tenuto dall'UIF, e alcune figure di intermediari che intervengono nel processo di erogazione del credito, approfittando della situazione di difficoltà dei richiedenti finanziamenti che non riescono ad accedere al sistema bancario. La Banca d'Italia richiede ai soggetti vigilati di segnalare le ipotesi di abusivismo e informa gli organi inquirenti dei casi di sospetta attività abusiva di cui ha notizia nell'esercizio delle attività di controllo. Si pone, più in generale, la questione se le forme di controllo previste sugli intermediari finanziari minori siano adeguate per assicurare piena correttezza nei confronti della clientela.

L'attuale normativa attribuisce all'UIF il compito di tenere l'elenco generale degli intermediari finanziari non bancari, di disciplinare le modalità di iscrizione, di esercitare minimali controlli, di verificare il rispetto della normativa in materia di trasparenza, di applicare sanzioni amministrative per un circoscritto numero di ipotesi e di proporre la cancellazione dell'intermediario dall'elenco.

Poteri ancora minori sono esercitabili nei confronti dei soggetti finanziari non operanti con il pubblico, dei Confidi, dei cambiavalute, dei mediatori creditizi e degli agenti in attività finanziaria che operano nel campo del money transfer. Gli schemi disciplinari mostrano una origine comune ma risultano molto differenziati: per alcuni soggetti sono previste solo forme di censimento; per altri velate forme di controllo e poteri di intervento finalizzati a esigenze di integrità. Le stesse finalità dei diversi interventi normativi divergono tra loro, fino ad apparire in alcuni casi sfuggenti. Peraltro la scarsa incidenza dei requisiti richiesti per l'accesso, spesso limitati solo all'onorabilità, e l'assenza di poteri di verifica dell'effettiva operatività svolta fanno sorgere dubbi sull'opportunità delle scelte legislative operate; l'iscrizione in albi può essere intesa dal pubblico quale "patente di legalità" per soggetti sui quali non opera in realtà un vaglio significativo e potrebbe, quindi, influire negativamente sulla trasparenza e correttezza complessiva del sistema.

2.13 Materie rilevanti ai fini della compliance: trasparenza delle operazioni e dei servizi bancari

Affinché la concorrenza fra intermediari possa svolgere pienamente la funzione di accrescere i servizi finanziari a disposizione delle fasce più deboli di imprese e famiglie e perché queste ultime possano effettuare scelte consapevoli è essenziale la trasparenza delle condizioni di offerta.

Essa richiede un'azione del regolatore a protezione del cliente, efficace e misurata. Una regolamentazione intrusiva irrigidisce il mercato e rischia di compromettere il raggiungimento delle stesse finalità a cui essa si ispira.

La tutela del cliente deve essere affidata soprattutto a strumenti che garantiscano una piena informazione sulle condizioni praticate e l'applicazione di un generale canone di correttezza nelle relazioni d'affari.

In alcuni casi particolari l'azione normativa può spingersi fino a proibire formule contrattuali che costituiscono un ostacolo oggettivo alla trasparenza delle condizioni o alla concorrenza, come le commissioni di massimo scoperto e le spese di chiusura dei conti.

Ma, in generale, interventi in favore della trasparenza non vanno confusi con forme di prezzi amministrati, che hanno un'elevata probabilità di ritorcersi, negli effetti concreti, contro le categorie di utenti che si cerca di tutelare. L'effettiva protezione del cliente deve contare anche su forme rapide ed economiche di tutela dei diritti.

I sistemi devono essere caratterizzati da imparzialità dell'organo preposto alla decisione e speditezza delle procedure di risarcimento del cliente.

Nessuna tutela formale è efficace se gli interessati non hanno sufficienti strumenti di valutazione. Perché gli utenti dei servizi bancari possano orientarsi tra prodotti finanziari diversi e a volte complessi occorre che abbiano una cultura finanziaria adeguata.

I punti focali della normativa sulla trasparenza dei servizi e prodotti bancari sono i seguenti:

- pubblicità delle condizioni delle operazioni e dei servizi offerti e informazione precontrattuale;
- il cliente che ha sottoscritto il contratto ha diritto di riceverne una copia comprensiva delle condizioni generali;
- gli intermediari hanno l'obbligo di fornire una informativa chiara e completa durante lo svolgimento del rapporto contrattuale e un quadro sempre aggiornato delle condizioni applicate.

Le informazioni oggetto delle norme di Trasparenza devono essere fornite alla clientela in modo corretto, chiaro ed esauriente, in applicazione del principio di proporzionalità, la disciplina si articola con modalità differenziate in relazione alle esigenze delle diverse fasce di clientela e alle caratteristiche dei servizi.

La disciplina sulla trasparenza presuppone che le relazioni d'affari siano improntate a criteri di buona fede e correttezza.

Per quanto concerne i controlli di conformità normativa, periodicamente, la Funzione Compliance verifica l'adeguatezza e l'efficacia delle procedure organizzative per rilevare eventuali carenze riscontrate e riferisce con periodicità almeno annuale agli organi aziendali.

La pubblicità delle operazioni, dei servizi offerti e delle relative condizioni contrattuali si basa sui seguenti strumenti:

- il documento contenente i "Principali diritti del cliente";
- il "Foglio informativo", contenente informazioni sull'intermediario, sulle condizioni e sulle principali caratteristiche dell'operazione o del servizio offerto;
- la copia completa dello schema di contratto, che può essere richiesta dal cliente prima della conclusione del contratto;
- il "Documento di sintesi" delle principali condizioni.

Il puntuale rispetto della Disciplina sulla Trasparenza delle condizioni contrattuali e l'efficace presidio dei rischi di natura legale e reputazionale connessi ai rapporti con la clientela richiedono l'adozione, da parte della Banca, di opportune modalità operative che assicurino:

- la valutazione della struttura dei prodotti offerti in relazione alla comprensibilità, da parte della clientela, della loro struttura, delle loro caratteristiche e dei rischi tipicamente connessi ai medesimi;

- la conformità a prescrizioni imperative di legge dei servizi o prodotti offerti;
- la trasparenza e la correttezza nella commercializzazione dei prodotti tramite una documentazione informativa completa e in modo che il cliente non sia indirizzato verso prodotti evidentemente inadatti rispetto alle proprie esigenze finanziarie.

Le vigenti norme di Legge (art. 128 Dlgs. 1° Settembre 1993, n. 385 – T.U.B.) attribuiscono alla Banca d'Italia la facoltà di effettuare visite ispettive presso il sistema bancario al fine di verificare il rispetto delle norme in materia di "Trasparenza Bancaria".

In caso di eventuale visita ispettiva da parte della Banca d'Italia, la filiale interessata deve darne immediata comunicazione alla Funzione Organizzativa di Area e al relativo Responsabile il quale poi, di concerto con il Responsabile della Funzione di Revisione Interna, deve individuare personale in grado di supportare gli ispettori medesimi per tutta la durata della verifica mediante la presenza presso la filiale interessata.

3 I RAPPORTI TRA LA FUNZIONE DI COMPLIANCE E LA FUNZIONE DI REVISIONE INTERNA

Le caratteristiche tipiche del rischio di compliance pongono la relativa funzione in posizione trasversale rispetto alle consuete attività di gestione dei rischi e di controllo interno, facendo nascere il problema di coordinare i nuovi strumenti di controllo con quelli già esistenti, anche se molto diversi a seconda delle varie realtà aziendali . A tal proposito, Hinna asserisce che: «il vero rischio è che il sistema dei controlli non sia "a sistema" ma a semplice sommatoria»; vale a dire che il concetto di rischio di non conformità deve essere considerato secondo un'accezione più ampia di quella usualmente proposta, tenuto conto che esso include non solo i rischi derivanti dalla mancanza di un presidio efficace su tutte le aree esposte, ma anche quelli prodotti dalle carenze nel coordinamento degli strumenti e delle strutture poste a presidio del rischio stesso.

Se, d'altro canto, si considera che lo sviluppo delle funzioni di controllo interno si è avuto spesso come reazione a eclatanti scandali finanziari, che hanno coinvolto le banche, e che hanno portato come conseguenza alla nascita di un certo numero di funzioni, la cui ripartizione dei compiti non è sempre chiaramente definita, si comprende il motivo dell'attenzione che è necessario porre riguardo alle possibili aree di sovrapposizione fra l'attività svolta dalla Funzione di Compliance e quella realizzata dalle altre funzioni di controllo interno, in particolare quella di Revisione Interna.

A tal fine, verranno analizzate in parallelo le attività e gli obiettivi della Funzione Compliance e della Funzione di Revisione Interna, inizialmente mediante un confronto delle definizioni maggiormente condivise a livello internazionale, e successivamente verranno esaminate le principali norme che prevedono l'istituzione di un'attività di compliance; così da evidenziare

i compiti e le caratteristiche attribuite da ognuna di esse alle diverse funzioni aziendali.

Il ragionamento trova forza nella considerazione che l'applicazione delle nuove disposizioni nazionali (la legge sul risparmio, la L. 231/2001 o la nuova legge sull'antiriciclaggio), così come delle direttive comunitarie e dei documenti emanati da Comitato di Basilea (Mifid e Direttive di applicazione, Nuovo Accordo di Basilea, disciplina sulla Funzione Compliance), hanno determinato la necessità di cambiamenti e di notevoli sforzi di adattamento, che, da una parte, dovranno essere tesi a valutare le ragioni della crescente sfiducia dei risparmiatori riguardo l'operato delle banche e a orientare, di conseguenza, l'organizzazione bancaria verso il conseguimento di più solidi rapporti fiduciari; mentre, dall'altra parte, dovranno prediligere il perseguimento della stabilità interna e il contenimento dei costi derivanti da comportamenti non-compliant.

In questa nuova visione dell'attività bancaria la corporate governance, il sistema dei controlli interni, le prassi operative e decisionali devono essere organizzate, coerentemente con gli obiettivi aziendali, tenendo conto della valorizzazione del requisito reputazionale, garantendo la funzionalità e l'indipendenza degli organi aziendali, la diffusione capillare di un sistema di valori condivisi, il rispetto delle norme e la valorizzazione di una Funzione di Compliance efficace ed efficiente.

Nel giugno del 1999 il Consiglio di Amministrazione dell'Institute of Internal Auditors approvava la seguente definizione di Internal Audit (Revisione Interna): "*L'Internal Auditing è un'attività indipendente e obiettiva di assurance e consulenza, finalizzata al miglioramento dell'efficacia e dell'efficienza dell'organizzazione. Essa assiste l'organizzazione nel perseguimento dei propri obiettivi tramite un approccio professionale sistematico, che genera valore aggiunto in quanto*

finalizzato a valutare e migliorare i processi di controllo, di gestione dei rischi e di corporate governance".

Dalla definizione riportata si evince che l'attività di Revisione Interna è prevalentemente individuabile nelle funzioni di *consulting* e *assurance*.

L'Associazione Italiana Internal Auditors (AIIA) definisce i servizi di assurance stabilendo che essi "*comportano un'obiettiva valutazione delle evidenze da parte dell'internal auditor, finalizzata all'espressione di un giudizio indipendente in merito a un processo, sistema, o altro*".

I servizi di consulenza sono definiti, altresì, come "*attività di supporto e assistenza, la cui natura ed estensione siano concordate con il cliente, intesi a fornire valore aggiunto e migliorare i processi di governance, risk management e controllo di un'organizzazione*".

L'AIIA specifica, inoltre, che nello svolgimento del suo compito "*l'auditor deve conservare la propria obiettività, senza assumere responsabilità di tipo manageriale*".

L'Internal Auditing non riveste, infatti, un ruolo decisionale.

I servizi di consulting devono essere definiti in un formale mandato, in cui siano riportate la natura, l'autorità e le responsabilità dell'Internal Audit.

I requisiti essenziali dell'attività di internal audit sono definiti nell'ambito degli Standard internazionali per la professione, recepiti in Italia dall'AIIA.

Negli standard della professione vengono definite le caratteristiche principali che debbono caratterizzare l'attività di revisione interna, in pratica declinano il livello minimo di prestazione atteso (tale livello è quello necessario ad ottemperare alle responsabilità assegnate). Essi si distinguono in:

- **Standard di Connotazione**: stabiliscono le caratteristiche che le organizzazioni e gli individui che svolgono attività di internal auditing, devono obbligatoriamente possedere (indipendenza, obiettività, competenza, diligenza professionale, etc.);
- **Standard di Prestazione**: descrivono la natura e le caratteristiche dell'attività di audit (gestione attività di audit, pianificazione e svolgimento incarichi, monitoraggio, etc.).

Gran parte dell'attività di consulenza, come si evince dalla stessa definizione, è la naturale estensione dei servizi di assurance e investigativi e può consistere in indicazioni, analisi e valutazioni formali o informali.

Le funzioni di assurance e di consulting non si escludono a vicenda e non precludono la possibilità di fornire ulteriori servizi, quali investigazioni e altre attività non riferibili al ruolo di revisore interno . A queste, infatti, si aggiunge normalmente l'attività di reporting verso il vertice aziendale, a cui si fa espresso riferimento negli Standard Internazionali per la professione di Internal Auditing, laddove si stabilisce che "*il Responsabile dell'Internal Auditing deve riportare a un livello dell'organizzazione che consenta il pieno adempimento delle proprie responsabilità*".

Nella guida interpretativa redatta dall'AIIA si stabilisce, a tal proposito, che il Responsabile dell'Internal Auditing (RIA) deve riferire al Comitato di Controllo Interno, o Organo equivalente, e si definiscono due livelli di riporto: il "riporto funzionale" e il "riporto gerarchico".

Attraverso il primo, il Responsabile Internal Auditing riferisce all'Organo di governo societario (il quale deve, fra l'altro, approvare il mandato dell'Internal Audit, ricevere le comunicazioni sui risultati dell'attività svolta dalla funzione, approvare le decisioni relative alla nomina e alla rimozione del Responsabile Internal Auditing).

Il riporto gerarchico, invece, è interno alla struttura di management e ha la funzione di facilitare l'operatività quotidiana della Funzione di Revisione Interna. In ogni caso, l'adempimento di tali attività deve essere effettuato nel rispetto dei principi di integrità, obiettività, riservatezza e competenza.

La definizione di Internal Audit appena riportata è a monte di un intero processo di evoluzione della figura professionale dell'internal auditor, che riveste un ruolo di "consulente interno", il cui contributo è finalizzato, come evidente, non più solo al controllo dei processi aziendali, così come era nell'ottica "della vecchia Funzione di Ispettorato", ma anche al loro continuo miglioramento.

Ciò che è cambiata è la filosofia sottostante la tipologia e le modalità operative dell'attività svolta; mentre l'ispettorato tradizionale aveva il compito di "individuare l'errore e chi l'ha commesso", l'auditor, una volta accertato l'evento in questione, deve invece comprendere le cause e la natura dell'errore e deve adoperarsi affinché possano essere identificate pratiche finalizzate al miglioramento del sistema aziendale di riferimento.

La sua funzione di consulente si coniuga, pertanto, con quella di "garante dell'efficienza e della funzionalità del sistema di controllo interno aziendale".

L'espansione dei contenuti delle Funzioni di Revisione Interna, da quelli tipici dell'ispettorato, di natura prettamente operativa (il cosiddetto controllo a norma), a quelli propri dell'attività di Internal Audit, più votati alla logica organizzativa e al sostegno nel raggiungere gli obiettivi aziendali con efficacia ed efficienza, si evincono, nella normativa nazionale, nelle Istruzioni di Vigilanza per le banche, predisposte dalla Banca d'Italia, che, a seguito del 145° aggiornamento[64], prevedono l'istituzione di una

[64] Istruzioni di Vigilanza per le Banche, "Sistema dei controlli interni, compiti del Collegio Sindacale", 145° Aggiornamento del 9 ottobre 1998 alla circolare n. 4 del 29 marzo.

"funzione indipendente", che svolga l'attività di revisione interna, e attribuisce a detta funzione la valutazione della funzionalità complessiva del Sistema di Controllo Interno (SCI) e il compito di "portare all'attenzione del Consiglio di Amministrazione e dell'alta direzione i possibili miglioramenti alle politiche di gestione dei rischi, agli strumenti di misurazione e alle procedure". Le tendenze evolutive di cui si parla sono ancora più evidenti in quei documenti che attribuiscono alla Funzione di Revisione Interna il controllo sui processi di compliance e fanno sorgere la necessità di definire puntualmente i compiti e le responsabilità di ognuna di esse, soprattutto là dove le due funzioni sembrano avere maggiori margini di sovrapposizione.

La stessa Guida Interpretativa per la pratica professionale, predisposta dall'Associazione Italiana degli Internal Auditors, a commento dello Standard 1110 (Indipendenza Organizzativa), riporta testualmente: «Il Responsabile della Funzione di Internal Audit deve anche tener conto dei propri rapporti con altre funzioni di monitoraggio e controllo (risk management, Compliance, sicurezza, legale, revisione esterna) e facilitare la segnalazione di rilevanti problematiche di rischio e controllo al comitato di controllo interno».

Il Comitato di Basilea per la Vigilanza Bancaria riporta a sua volta che: "*The bank's board of directors has the ultimate responsibility for ensuring that senior management establishes and maintains an adequate and effective system of internal controls, a measurement system for assessing the various risks of the bank's activities, a system for relating risks to the bank's capital level, and appropriate methods for monitoring compliance with laws, regulations, and supervisory and internal policies*".

In questo documento, come evidente, si fa esplicito riferimento al compito di predisporre adeguati metodi per monitorare l'attività di conformità a

leggi, regolamenti e politiche interne; tale attività viene affiancata a quella di assurance del sistema dei controlli interni e di verifica sui sistemi di valutazione dei rischi aziendali e dell'adeguatezza patrimoniale; contribuendo ad ampliare ulteriormente le competenze dell'Internal Auditing.

Una puntuale definizione di "Compliance Function" viene proposta nell'aprile del 2005 dal Comitato di Basilea che, nel più volte menzionato documento "Compliance and compliance function in bank", stabilisce testualmente che essa consiste in: "*An independent function that identifies, assesses, advises on, monitors and reports on the bank's compliance risk, that is, the risk of legal or regulatory sanctions, material financial loss, or loss to reputation a bank may suffer as a result of its failure to comply with laws, regulations, rules, related self-regulatory organisation standards, and codes of conduct applicable to its banking activities*", l'espressione "*compliance function is used to describe staff carrying out compliance responsibilities*".

E' evidente, dunque, che relativamente ai rischi di non conformità, la funzione deve:

- attuarne l'identificazione;
- definire le procedure di monitoraggio e di controllo;
- offrire supporto consultivo alle strutture aziendali;
- seguire lo sviluppo delle normative nazionali ed internazionali;
- formulare il reporting destinato agli organi amministrativi e di controllo dell'azienda;
- mantenere i rapporti con gli Organi di Vigilanza e con le Autorità;
- coordinare e intervenire nell'attività di formazione e di sensibilizzazione del personale, promuovendo lo sviluppo della cultura etica e deontologica e di controllo.

Detta funzione si inserisce a pieno titolo nel quadro complessivo del sistema dei controlli interni (di cui le banche si dotano ai sensi del Titolo IV, Capitolo 11, Sezione II delle Istruzioni di Vigilanza) con l'obiettivo di "controllare e gestire il rischio di non conformità". La definizione di compliance appena proposta, può presentare elementi di sovrapposizione con l'attività di Revisione Interna; infatti, pure per la Funzione compliance si prevede un'attività di consulenza, assurance e verifica, anche se finalizzata alla gestione e al controllo del solo rischio di non conformità.

Il processo di compliance coinvolge altresì diverse funzioni e organi aziendali, durante le varie fasi che lo caratterizzano; in ognuna di queste fasi è possibile che si verifichino sovrapposizioni e inefficienti duplicazioni di costi. Appare utile, dunque, analizzare le principali fonti normative che si richiamano a un'attività di conformità o che possono essere incluse nel perimetro di competenza della compliance, per individuare i compiti specifici e il campo di applicazione delle funzioni attribuite ai diversi organi, nonché l'esistenza di possibili rischi di duplicazioni di processi o procedure.

La direttiva della commissione europea 2004/39/CE, nota come Markets in Financial Instruments Directive (MiFID), ha come obiettivo principale quello di contribuire alla creazione di un mercato finanziario europeo integrato, in cui tutti gli investitori godranno dello stesso livello di protezione e in cui sia garantita l'efficienza, la trasparenza e l'integrazione delle infrastrutture di negoziazione.

In conseguenza delle nuove richieste di trasparenza si viene a modificare il ruolo assunto dalle funzioni di controllo nelle banche, in particolare delle funzioni di compliance, revisione interna e risk management.

La direttiva recante modalità di esecuzione della MiFID per quanto riguarda i requisiti di organizzazione e le condizioni di esercizio dell'attività delle

imprese di investimento contiene regole più precise e misure tecniche per l'applicazione dei principi generali dettati dalla MiFID.

Il Capo II, titolato "Requisiti di organizzazione", stabilisce, all'art. 5 comma 1, lettera a) che, compatibilmente con la natura, le dimensioni e la complessità dell'attività svolta, nonché con il tipo e la gamma dei servizi di investimento prestati, le banche e le imprese di investimento devono «istituire, applicare e mantenere procedure decisionali e una struttura organizzativa che specifichi in forma chiara e documentata i rapporti gerarchici e la suddivisione delle funzioni e delle responsabilità»; ai punti successivi si richiama la necessità di idonei meccanismi di controllo interno, finalizzati a «garantire il rispetto delle decisioni e delle procedure a tutti i livelli dell'impresa d'investimento», specificando che il personale impiegato in queste attività sia «provvisto delle qualifiche, delle conoscenze e delle competenze necessarie per l'esercizio delle responsabilità loro attribuite».

Gli articoli seguenti (art. 6, 7, 8) sono dedicati rispettivamente alla "compliance", al "risk management" e all'attività di "internal audit"; in tal modo la direttiva contribuisce a definire le funzioni aziendali maggiormente coinvolte nel processo di applicazione dei principi della MiFID.

L'art. 6, comma 1, § 1, stabilisce che le imprese di investimento devono «istituire, applicare e mantenere politiche e procedure adeguate per individuare il rischio di mancata osservanza degli obblighi di cui alla direttiva MiFID da parte dell'impresa, nonché i rischi che ne derivano, e devono mettere in atto politiche e procedure idonee per minimizzare tale rischio e consentire alle autorità competenti di esercitare efficacemente i poteri conferiti loro dalla direttiva». A tali fini, secondo quanto riportato nel successivo comma 2, «le imprese di investimento devono tenere conto della natura delle dimensioni e della complessità della loro attività» e istituire una

funzione di compliance che sia permanente, efficace, indipendente (art. 6, § 2) e abbia il compito di controllare e valutare regolarmente l'adeguatezza e l'efficacia delle misure e delle procedure adottate per individuare e minimizzare il rischio di mancata osservanza degli obblighi derivanti dalla MiFID e assicurare alle autorità competenti di poter esercitare efficacemente i loro poteri. Ad essa è attribuito, inoltre, il controllo e la valutazione dell'adeguatezza e dell'efficacia delle misure adottate per rimediare ad eventuali carenze nell'adempimento degli obblighi, nonché il compito di «fornire consulenza e assistenza ai soggetti rilevanti incaricati dei servizi di investimento e delle attività di investimento ai fini dell'adempimento degli obblighi previsti dalla direttiva» (art. 6, § 2, b)).

Le condizioni che devono essere soddisfatte affinché si consenta alla Funzione di Compliance di svolgere i suoi compiti con correttezza e indipendenza sono definite all'art. 6, §3, che riporta testualmente:

- la Funzione di Compliance deve disporre dell'autorità, delle risorse e delle competenze necessarie e avere adeguato accesso alle informazioni pertinenti;
- deve essere nominato un responsabile per la Funzione di Compliance, al quale spetta il compito di presentare le relazioni almeno una volta l'anno in merito all'attività di compliance svolta e alle misure adottate per rimediare a eventuali carenze;
- i soggetti rilevanti che partecipano alla funzione di compliance non devono partecipare alle prestazioni di servizi e all'esercizio delle attività che sono chiamati a controllare (principio di separatezza);
- la remunerazione dei soggetti rilevanti che partecipano alla funzione di compliance non deve comprometterne l'obiettività.

Relativamente all'attività di internal audit, l'art. 8, § 1 stabilisce che «le imprese di investimento, se ciò è opportuno e proporzionato, vista la natura,

le dimensioni e la complessità dell'attività d'impresa (…) istituiscano e mantengano una funzione di audit interno separata e indipendente dalle altre funzioni e attività dell'impresa di investimento», con il compito di:

- adottare, applicare e mantenere un piano di audit per l'esame e la valutazione dell'adeguatezza e dell'efficacia dei sistemi, dei meccanismi di controllo interno e dei dispositivi dell'impresa di investimento;
- formulare raccomandazioni sulla base dei risultati dei lavori realizzati;
- verificare l'osservanza di tali raccomandazioni;
- relazionare, almeno annualmente, sulle questioni relative all'audit interno.

Gli articoli appena indicati descrivono l'attività delle due funzioni distinguendola in almeno quattro tipologie comuni ad entrambe: l'attività generale di controllo, l'attività di consulenza, di assurance e di reporting.

Il dettato della norma, in ogni modo, non prende in considerazione la possibilità di sovrapposizioni, infatti, sottolinea più volte la necessaria indipendenza di entrambe le funzioni; in maniera particolare, quando fa riferimento alla Revisione Interna, riporta testualmente che essa deve essere "separata e indipendente dalle altre funzioni e attività dell'impresa".

Tali disposizioni possono indurci a ritenere che la volontà del legislatore, in questo contesto, sia quella di ricondurre l'attività di compliance a una attività di gestione del rischio (di un rischio particolare, reputazionale e strategico, non facilmente quantificabile né gestibile con le consuete procedure) proprio come la funzione di risk management (la cui descrizione, infatti, è riportata al seguente art. 7); mentre quella di internal audit si prefigura come un'attività concernente i sistemi e i meccanismi di

controllo interno nel loro insieme e, in quanto tale, concernente anche il controllo della Funzione compliance.

La stessa disposizione degli articoli, che sotto la comune etichetta "Organisational requirements", riporta in ordine:

- art. 5 "General organisational requirements";
- art. 6 "Compliance";
- art. 7 "Risk management";
- art. 8 "Internal audit";

sembra rispecchiare questa interpretazione, nell'intento di voler individuare due diversi livelli di controllo: il primo compiuto, per le attività di rispettiva competenza, dalle funzioni che gestiscono il rischio di non conformità e le altre tipologie di rischi tipici dell'attività di investimento; il secondo compiuto dalla Funzione di Revisione Interna, finalizzato a *«examine and evaluate the adequacy and effectiveness of the investment firm's systems, internal control mechanisms and arrangements».*

Invece, con il D.Lgs. n. 231/2001 il legislatore è intervenuto sull'organizzazione aziendale allo scopo di diffondere una cultura della legalità in ambito societario, prevedendo delle sanzioni per quegli enti o società i cui "soggetti apicali", o persone sottoposte alla direzione o alla vigilanza di questi ultimi, abbiano commesso reati nell'interesse o a vantaggio degli stessi enti (art. 5, d.lgs 231/2001). Presupposto affinché si possa applicare la disciplina in questione è che l'illecito sia stato compiuto "nell'interesse o a vantaggio" dell'ente.

E' evidente dal dettato normativo che, mentre nel primo caso si fa riferimento ad un difetto nella volontà dell'agente, nel secondo caso ciò che ha valore è l'effettivo risultato della condotta illecita.

La responsabilità dell'ente non sussiste quando l'illecito è compiuto nonostante siano stati adottati e attuati i modelli di gestione atti a prevenire tali reati; quando il compito di vigilare sul funzionamento e l'osservanza dei modelli è affidato ad un organismo con autonomi poteri di iniziativa e di controllo; quando gli agenti abbiano eluso fraudolentemente i modelli di organizzazione e gestione. Da qui l'importanza di pervenire all'individuazione di un organismo ad hoc e di armonizzare la sua attività e la sua struttura con le altre già presenti nelle banche.

I modelli di organizzazione e di gestione dei rischi derivanti dai diversi segmenti operativi sono introdotti all'art. 6 del decreto in esame; in particolare al secondo comma sono elencate le attività che sono chiamati a svolgere:

- individuare le attività nel cui ambito possono essere commessi reati;
- prevedere specifici protocolli diretti a programmare la formazione e l'attuazione delle decisioni dell'ente in relazione ai reati da prevenire;
- individuare modalità di gestione delle risorse finanziarie idonee ad impedire la commissione dei reati;
- prevedere obblighi di informazione nei confronti dell'organismo deputato a vigilare sul funzionamento e l'osservanza dei modelli;
- introdurre un sistema disciplinare idoneo a sanzionare il mancato rispetto delle misure indicate nel modello.

Il successivo art. 7 al comma 3 stabilisce che «il modello prevede, in relazione alla natura e alla dimensione dell'organizzazione, nonché al tipo di attività svolta, misure idonee a garantire lo svolgimento dell'attività nel rispetto della legge e a scoprire ed eliminare tempestivamente le situazioni di rischio». L'organismo di controllo "dell'ente", direttamente incaricato di vigilare sul funzionamento, l'osservanza e l'aggiornamento dei modelli, deve godere di "autonomi poteri di iniziativa e di controllo", pertanto

sembrerebbe che tale centro di potere non possa essere individuato in un organo come il Collegio Sindacale o come gli Uffici Legali o le Segreterie Generali, essendo queste ultime "gerarchicamente incardinate"23, né in organi esterni alla banca, come le società di revisione, perché non sono dotati dei poteri richiesti (autonomia di iniziativa e di controllo). Sarà necessario, dunque, individuare una funzione ad hoc, che disponga di un budget idoneo all'attività da svolgere e di poteri di controllo e vigilanza atti ad effettuare le verifiche richieste per contenere i rischi derivanti dal compimento degli illeciti elencati.

Naturalmente, i modelli organizzativi descritti devono tenere in considerazione la specifica struttura aziendale e le dimensioni medie della banca; il decreto stesso, infatti, al quarto comma dell'art. 6, stabilisce che negli enti di piccole dimensioni tali compiti possono essere direttamente affidati all'organo dirigente. A tal proposito, le Linee Guida dell'Associazione Bancaria Italiana (ABI) per l'adozione di modelli organizzativi sulla responsabilità amministrativa delle banche, pubblicate nel febbraio del 2004, al Capitolo II, § 1.3, ribadiscono che «l'adozione dei modelli organizzativi è una facoltà della banca e, come tale, può essere adempiuta secondo modalità che variano da banca a banca, a seconda delle sue dimensioni, dell'attività svolta e della connessa valutazione costi/benefici».

Il modello organizzativo (Capitolo II, § 2.1) deve essere dotato di autonomi poteri di iniziativa e di controllo, e ogni banca può valutare l'opportunità di creare una funzione ad hoc ovvero utilizzare un organismo o una funzione già esistente, «avendo cura di evitare che possano determinarsi sovrapposizioni di compiti e purché ne sia garantita l'autonomia e l'indipendenza».

L’ABI esclude al successivo paragrafo (Capitolo II, § 2.2) che si possa far riferimento ad un soggetto esterno, considerato che il decreto fa espresso richiamo a “l’organismo dell’ente”, ma riconosce la possibilità che questo possa servirsi della collaborazione di soggetti esterni.

Riguardo alle regole di funzionamento dell’organismo e ai requisiti dei suoi componenti, l’ABI individua i seguenti elementi (Capitolo II, § 2.4):

Compiti dell'organismo, in quanto organismo di controllo:

- vigilare sul funzionamento e l'osservanza dei modelli;
- curare il loro aggiornamento.

Requisiti dell'organismo:

- autonomi poteri di iniziativa e di controllo;
- personale qualitativamente e quantitativamente adeguato.

Poteri dell'organismo:

- disporre di un budget idoneo;
- poter colloquiare alla pari, senza vincoli di subordinazione gerarchica;
- essere dotato di poteri di richiesta ed acquisizione di informazioni da e verso ogni livello e settore della banca;
- poter costituire, in ragione della professionalità ed indipendenza dei propri componenti, un riferimento credibile;
- poter essere il soggetto cui la banca affida il compito di accertare i comportamenti e proporre le eventuali sanzioni a carico dei soggetti che non abbiano rispettato le prescrizioni contenute nel modello organizzativo e gestionale.

Nel Capitolo II, § 2.3, l’ABI, tenuto conto degli elementi fin qui esposti, individua alcune possibili soluzioni organizzative:

- Creare una funzione ad hoc costituita sia da professionalità interne alla banca (come legali, esperti contabili, di gestione del personale, di controllo interno nonché, ad esempio, un membro del collegio sindacale) che esterne ad essa (consulenti, esperti di revisione, ecc.), con la presenza di uno o più amministratori non esecutivi (o indipendenti).
- Identificare l'organismo di controllo con l'internal auditing che, eventualmente integrato nei poteri e nella composizione, può risultare adeguato ai compiti che il legislatore attribuisce all'organismo di controllo.
- Attribuire detta funzione di controllo ad un organismo composto da soli amministratori non esecutivi o indipendenti, secondo il modello, già noto alle banche quotate, del comitato di audit.

Le possibili soluzioni organizzative proposte dall'ABI sembrano essere state ricondotte prevalentemente alla presenza di una funzione apposita, che in alcuni casi è stata individuata nella Funzione di compliance (a) o all'ampliamento dei compiti dell'Internal Audit (b), a seconda delle dimensioni e dell'attività della banca.

Qualora la banca scelga di trasferire alla Funzione di Revisione Interna le competenze di cui al D.Lgs. 231/2001, in presenza di una contestuale Funzione di compliance, che si occupa della gestione dei rischi di non conformità, è possibile che si creino sovrapposizioni di competenze, quanto meno per l'analisi di quei comportamenti da cui possono derivare, direttamente o indirettamente, responsabilità amministrative della banca e sanzioni di qualsiasi genere che siano sottoposte all'attenzione della Compliance.

Se al contrario, si opta per adottare una Funzione compliance che includa anche i compiti e le responsabilità previste dal D. Lgs. 231/2001, l'internal

audit potrebbe continuare ad operare sui controlli di sistema, con un più ridotto rischio di sovrapposizione.

In questo secondo caso le disposizioni previste per adeguarsi al D. Lgs. 231/2001 potrebbero essere più agevolmente ricondotte a quelle stabilite direttiva MiFID. Nell'ipotesi, infine, in cui l'attività di cui al D.Lgs. 231/2001 sia svolta da una terza Funzione indipendente (ipotesi più accreditata fra le banche) questa potrebbe essere più agevolmente sottoposta ai "due livelli" di controllo esercitati, nell'ambito delle rispettive competenze, dall'attività di compliance e da quella di auditing, ma si renderebbe necessaria una chiara ed oggettiva attribuzione dei compiti e delle responsabilità fra le tre funzioni coinvolte.

Da quanto brevemente commentato è evidente come le scelte organizzative liberamente adottate dalle banche influenzeranno la presenza di rischi di sovrapposizione fra le due attività.

La legge 262/200525 nota come "legge sul risparmio" entra a far parte del perimetro di competenze dell'attività compliance, andando a modificare alcune disposizioni contenute nel Testo Unico della finanza, che è risultato essere il primo riferimento normativo oggetto dell'attività di verifica della conformità, secondo quanto emerso dall'indagine empirica.

La legge sul risparmio va ad ampliare l'attività di competenza della Funzione di Revisione Interna, attribuendogli delle competenze e delle responsabilità che ne influenzano l'assetto operativo e organizzativo, e, intervenendo sulla informativa societaria, produce riflessi sul sistema di controllo interno.

Per mezzo della legge sul risparmio il legislatore ha proceduto a rafforzare il sistema dei controlli sull'informativa economico finanziaria, attraverso la definizione di meccanismi formali di assunzione delle responsabilità (dichiarazione/attestazione) delle seguenti figure aziendali:

- gli “Organi amministrativi delegati”, ai quali si conferisce l’obbligo di redigere un’attestazione da allegare al bilancio di esercizio e consolidato circa l’adeguatezza e l’effettiva applicazione delle procedure amministrative e contabili, nonché la corrispondenza del bilancio alle risultanze dei libri e delle scritture contabili;
- il “Direttore Generale”, al quale spetta l’obbligo di dichiarare per iscritto la corrispondenza al vero delle informazioni e dei dati sulla situazione economica, patrimoniale e finanziaria previsti dalla legge e dal mercato;
- il “Dirigente preposto alla redazione dei documenti contabili societari” (in linea di massima identificabile con il CFO/Direttore Amministrazione Finanza e Controllo), che ha la responsabilità di predisporre adeguate procedure amministrative e contabili per la redazione del bilancio di esercizio e, ove previsto, del bilancio consolidato, nonché di ogni altra comunicazione di carattere finanziario; inoltre, anche in questo caso, è prevista l’attestazione, con apposita relazione allegata al bilancio d’esercizio o consolidato, dell’adeguatezza e dell’effettiva applicazione delle procedure amministrative e contabili nel corso dell’esercizio cui si riferisce il bilancio, nonché della corrispondenza del bilancio alle risultanze dei libri e delle scritture contabili. A fronte di queste disposizione di legge, le società interessate dovranno intraprendere un necessario processo di allineamento organizzativo, che includerà azioni finalizzate a:
- l’analisi degli impatti della legge su ruoli e responsabilità degli Organi amministrativi delegati e della figura del Direttore Generale (ove esistente);
- l’identificazione della figura del Dirigente preposto alla redazione dei documenti contabili societari ed il connesso conferimento di

adeguati poteri e mezzi per l'espletamento delle nuove responsabilità definite per Legge;

- la definizione dei rapporti tra il Dirigente preposto alla redazione dei documenti contabili societari e gli organismi preposti al controllo (ovvero Collegio Sindacale, Comitato di Controllo Interno, funzione Internal Audit, ecc.);
- l'esplicitazione, all'interno dell'organizzazione aziendale, delle responsabilità relative "al fare" e "al controllare". A fronte della "formale" identificazione dei responsabili finali delle comunicazioni societarie, sarà necessaria una "sostanziale" identificazione delle responsabilità di produzione delle informazioni che partono dai processi di business.

La Funzione di internal audit è chiamata a svolgere, in applicazione del dettato legislativo, un ruolo di assistenza al management, come esplicitamente richiesto dalla norma.

In merito, l'Associazione Italiana Internal Auditors (AIIA) ha pubblicato nel settembre del 2005 un position paper dal quale "(…) è possibile individuare le diverse funzioni e i ruoli che l'Internal Auditing può svolgere:

- può fornire un'importante funzione consultiva o può assistere l'organizzazione aziendale nell'identificare, valutare e implementare il sistema di gestione dei rischi e di controllo;
- può, grazie alla propria indipendenza ed autonomia, svolgere attività di controllo, analisi e verifica, fornendo i propri risultati alla linea manageriale;
- può svolgere, grazie alle sue competenze, attività di formazione in materia di controllo interno, risk assessment e valutazione dell'efficacia/efficienza dei controlli stessi;

- può essere fonte di competenze e metodi da trasmettere per processi strutturati di autodiagnosi aziendale del sistema di controllo dei processi (Control Risk Self Assessment");
- può formulare pareri oggettivi - basati su opportune evidenze di audit - sull'adeguatezza dei controlli implementati nella predisposizione del bilancio e dell'informativa finanziaria.

Tali attività potranno costituire utili strumenti di valutazione per il Dirigente preposto alla redazione dei documenti contabili societari nell'assunzione delle proprie responsabilità, nonché per il Comitato per il Controllo Interno, ove costituito (…)".

L'attività di internal audit risulta ampliata, come indicato, anche alla disciplina sul risparmio, con funzioni di controllo, di consulenza, attestazione e formazione che naturalmente implicano un rischio di sovrapposizione con l'attività di compliance, laddove essa sia chiamata a verificare la conformità delle prassi operative ai requisiti previsti dalla legge 262/2005, attraverso la consueta attività di verifica, di assurance e di consulting.

In tema di attività di consulenza, ad esempio, le due funzioni sono spesso chiamate a fornire pareri nei confronti dei soggetti "apicali", ma da quanto riportato nel position paper dell'AIIA, sembrerebbe che le valutazioni fornite dall'Internal Audit siano prevalentemente riferite al corretto ed efficiente funzionamento dei sistemi di controllo e di gestione dei rischi (e quindi anche della funzione di conformità), mentre alla Compliance spetterebbe il compito, se la disciplina entra nel suo perimetro di attività secondo mandato, di verificare l'aderenza delle prassi operative aziendali alle norme previste, al fine di non incorrere in sanzioni o multe. E' possibile individuare, pertanto, anche in questo contesto, due diversi livelli di controllo: il primo compiuto sulle singole discipline dall'attività di

compliance; il secondo compiuto sull'intero sistema dei controlli e di gestione dei rischi dall'Internal Audit.

4 LA FUNZIONE DI COMPLIANCE IN BANCA, UN CASO PRATICO: "LA NOSTRA BANCA"

4.1 Premessa

Al fine di fornire un quadro completo dell'architettura del Sistema dei Controlli Interni e soprattutto per definire un focus specifico relativo alla suddivisione delle attività tra Funzione di Compliance e Funzione di Revisione Interna, di seguito forniamo una sintetica rappresentazione della soluzione adottata da un intermediario creditizio nazionale.

Per motivi di riservatezza aziendale, legati anche alla sensibilità delle informazioni trattate, chiameremo nel corso della trattazione: LA NOSTRA BANCA.

Nel modello organizzativo vigente presso la Nostra Banca, gli Organi di Vertice sono i seguenti:

- il Consiglio di Amministrazione, con funzioni di supervisione strategica e gestione;
- il Comitato Esecutivo con funzioni di gestione, di tipo esecutivo, secondo i poteri delegati dal Consiglio di Amministrazione e attribuiti dallo Statuto;
- l'Amministratore Delegato con funzioni di gestione, di tipo esecutivo, secondo i poteri delegati dal Consiglio di Amministrazione e attribuiti dallo Statuto;
- il Direttore Generale, con funzioni di gestione di tipo esecutivo. In caso di assenza o impedimento del Direttore Generale le funzioni dello stesso sono assolte dal Vice Direttore Generale Vicario;
- il Collegio Sindacale con funzione di controllo.

4.2 Ruolo e compiti della Funzione di Compliance

La funzione di compliance presso la "Nostra Banca" possiede i requisiti richiesti dalle Autorità di Vigilanza ovvero:

- indipendenza, attraverso la formalizzazione del mandato della funzione ed attraverso la nomina di un responsabile indipendente;
- dotata di autorità e risorse qualitativamente e quantitativamente adeguate ai compiti da svolgere in relazione alla propria dimensione ed operatività[65].

La sua mission aziendale si può sintetizzare come segue: "*Assolvere alla funzione di controllo di conformità e alla funzione Antiriciclaggio; gestire le contestazioni extragiudiziali dei clienti e valutare la qualità del servizio erogato alla clientela"*.

La Funzione di Compliance riporta direttamente al Direttore Generale o all'Amministratore Delegato. Trasmette i flussi informativi verso gli Organi di Vertice aziendale, secondo la definizione nelle policy interne della Banca. Inoltre produce una rendicontazione periodica al Consiglio di Amministrazione sullo stato di conformità e presentazione annuale del piano degli interventi di mitigazione dei rischi (Compliance Plan).

Alla Funzione di Compliance è consentito l'accesso a tutte le attività aziendali svolte sia presso le strutture centrali sia presso le strutture periferiche nonché a qualsiasi informazione aziendale rilevante per lo svolgimento dei propri compiti, anche attraverso il colloquio diretto con il personale.

[65] Il personale che svolge funzioni di conformità deve essere adeguato per numero, competenze tecnico-professionali e aggiornamento, anche attraverso l'inserimento in programmi di formazione nel continuo.

Il Responsabile della funzione di Compliance possiede requisiti adeguati di indipendenza, autorevolezza e professionalità.

La nomina e la revoca del Responsabile della Compliance sono di competenza, esclusiva e non delegabile, del C.d.A. sentito il Collegio Sindacale, previo parere del Comitato per il Controllo Interno (ove presente), su proposta del Presidente. In tale ambito, la revoca può avvenire implicitamente attraverso la nomina di un nuovo Responsabile.

Lo stesso Consiglio di Amministrazione, sentito il Comitato per il controllo interno, determina l'assetto retributivo del Responsabile della Funzione di Compliance.

La nomina e l'eventuale revoca del Responsabile della Funzione di Compliance deve essere comunicata alla Banca d'Italia e, qualora previsto, alle altre Autorità di Vigilanza.

A livello organizzativo, presso la Funzione di Compliance della "Nostra Banca" sono previste 3 strutture di secondo livello che si occupano specificatamente degli aspetti afferenti la gestione del rischio di non conformità:

- Struttura Antiriciclaggio
- Struttura Materie di Compliance
- Struttura Reclami.

4.3 Ruolo e compiti della Funzione di Revisione Interna

La Funzione di Revisione Interna presso la "Nostra Banca" è collocata a diretto riporto degli Organi Amministrativi di Vertice.

La sua mission aziendale è la seguente: "*Verificare, in maniera indipendente, la regolarità dell'operatività e l'andamento dei rischi e valutare la funzionalità del complessivo sistema dei controlli interni, al fine di perseguire anche il miglioramento dell'efficacia e dell'efficienza dell'organizzazione. Validare le policy aziendali e il Regolamento che disciplina l'assetto organizzativo della Banca sotto il profilo del presidio dei rischi e di adeguatezza, efficacia e funzionalità del complessivo sistema dei controlli interni."*

L'Area Revisione Interna riporta gerarchicamente al Consiglio di Amministrazione, comunica direttamente i risultati delle attività di revisione e le valutazioni agli Organi di Controllo. La Funzione ha accesso ai dati aziendali e a tutte le attività, comprese quelle esternalizzate, svolte dalla Banca.

L'autonomia e l'indipendenza sono assicurate da meccanismi relazionali e di raccordo con gli Organi Collegiali aventi funzioni di supervisione strategica, gestione e controllo. In particolare:

- nomina/revoca e determinazione dell'assetto retributivo del Responsabile della funzione di Revisione Interna da parte del Consiglio di Amministrazione, su proposta dell'Amministratore incaricato del sistema di controllo interno e di gestione dei rischi, in condivisione con il Presidente del Consiglio di Amministrazione, previo parere favorevole del Comitato Controllo e Rischi, nonché sentito il Collegio Sindacale;
- determinazione dell'Audit Plan da parte del Consiglio di Amministrazione su relazione dell'Area Revisione Interna e previo esame degli Organi di Controllo;
- possibile attivazione delle revisioni interne da parte degli Organi di Controllo, del Comitato Controllo e Rischi, dell' ODV 231/2001, del

Presidente del CdA ed anche da parte dell'amministratore incaricato del sistema di controllo interno e di gestione dei rischi;

- rendicontazione dell'attività agli Organi di Controllo e almeno annualmente una relazione sulla valutazione sul sistema dei controlli al Consiglio di Amministrazione;
- composizione e dimensionamento della struttura da parte del Consiglio di Amministrazione, sulla base della relazione dell'Area Revisione Interna, previo parere degli Organi di Controllo;
- approvazione da parte del Consiglio di Amministrazione delle linee guida cui ispirare la gestione delle risorse destinate alla funzione di Revisione Interna (selezione, formazione, sistema premiante) e delle risorse economiche assegnate, sulla base della relazione dell'Area Revisione Interna, previo parere degli Organi di Controllo.

4.4 Rapporti tra Compliance e Funzioni Aziendali, con focus sui rapporti con la Revisione Interna

Per il corretto esercizio delle responsabilità assegnate la funzione di Compliance collabora con le altre funzione aziendali allo scopo di sviluppare le proprie metodologie di gestione del rischio in modo coerente con le strategie e l'operatività aziendale e prestando ausilio consultivo.

In particolare, nell'ambito delle competenze assegnate dalle policy aziendali le diverse funzioni aziendali assicurano idonei flussi informativi in input/output alla funzione di Compliance. In particolare:

- Legale, per l'interpretazione delle evoluzioni legislative;
- Organizzazione, per gli adeguamenti organizzativi necessari;

- Risk Management, per lo sviluppo del modello di gestione dei rischi di non conformità e la valutazione periodica (misurazione e mitigazione) degli stessi;
- Revisione Interna, sui risultati delle attività di controllo.

La funzione di Revisione informa altresì la funzione di compliance su eventuali rischi di conformità rilevati nel corso dell'attività di internal audit per l'esercizio delle responsabilità di competenza e l'attivazione e monitoraggio delle opportune iniziative.

Al fine di rappresentare al meglio il modello organizzativo vigente presso la "Nostra Banca" di seguito si descrive il processo di gestione del rischio di non conformità adottatto dall'intermediario oggetto del nostro caso aziendale.

Il processo di gestione del rischio di non conformità è composto da 5 fasi principali:

- identificazione dei cambiamenti normativi e loro impatto;
- valutazione stato di conformità;
- sviluppo intervento di adeguamento;
- gestione anomalie di conformità;
- informativa verso gli organi di vertice;
- comunicazione e formazione;
- supporto ed assistenza;
- revisione interna.

Identificazione dei cambiamenti normativi e loro impatto: il processo ha l'obiettivo di identificare nel continuo l'evoluzione della normativa di riferimento e di valutarne l'impatto su processi e procedure aziendali. La funzione di Compliance ha il compito di attivare le funzioni responsabili dell'implementazione successiva e predisporre lo "scadenziario " degli adeguamenti richiesti dalle norme.

La funzione Legale fornisce supporto sia in termini di segnalazioni sull'evoluzione legislativa che in termini di interpretazione della stessa.

valutazione stato di conformità: il processo ha l'obiettivo di verificare, nel continuo o a evento e comunque almeno annualmente, la situazione di conformità del sistema aziendale rispetto alla normativa esterna.

Per definire il quadro complessivo "dello stato di conformità" ed individuare le necessità di modifica organizzativa e procedurale, la Funzione di Compliance produce produce la reportistica sulla situazione di conformità e la proposta degli interventi di mitigazione per gli Organi di Vertice effettuando in merito il monitoraggio dell'effettiva realizzazione degli interventi, sulla base anche del contributo ricevuto dalle seguenti funzioni aziendali:

- Risk Management per l'analisi quantitativa delle perdite e dei rischi potenziali di non conformità;
- Revisione Interna per l'analisi sulle attività di controllo effettuate e le criticità/violazioni emerse;
- Organizzazione per l'analisi di soluzioni di mitigazione.

Inoltre il Responsabile Compliance segnala al Comitato per il Controllo Interno la necessità di specifiche attività di verifica sulle aree che sono maggiormente esposte al rischio ovvero le esigenze di controllo di conformità dei comportamenti aziendali alle regole aziendali definite. In tali circostanze, il Comitato per il Controllo richiede alla funzione di Revisione Interna di integrare il Piano di Audit con le richieste del Responsabile della Compliance. Su tali indicazioni fornisce informativa alla Direzione Generale e agli Organi Aziendali.

La funzione di Revisione Interna informa la funzione di Compliance circa le effettive integrazioni delle richieste all'interno del Piano di Audit.

Il controllo e la valutazione dell'adeguatezza e dell'efficacia delle procedure adottate ai sensi della regolamentazione di vigilanza in materia di prestazione dei servizi di investimento, sono forniti dalla funzione di Revisione Interna. La funzione di Compliance può svolgere autonomamente verifiche, in caso di necessità su particolari aree di analisi, al fine di accertare l'effettiva applicazione dei controlli di conformità previsti sulle procedure e l'idoneità dei modelli organizzativi adottati.

sviluppo intervento di adeguamento: il processo ha l'obiettivo di implementare gli interventi de finiti nel piano di mitigazione del rischio di non conformità o scaturiti nel continuo dal governo dei processi, pervenendo al rilascio delle procedure organizzative (normativa interna, applicazioni informatiche, processi operativi, formazione, controlli,…). La funzione Organizzazione per gli ambiti di competenza costituisce il punto di riferimento per la gestione dei progetti definiti nel piano di mitigazione coordinando i lavori fornendo informativa andamentale alla funzione di Compliance.

La funzione di Compliance certifica la rispondenza delle soluzioni di volta in volta individuate per l'avvio in operativo.

L'attività di certificazione viene svolta anche con riferimento a:

– iniziative progettuali interne non direttamente correlate ad evoluzioni legislative ma aventi significativi impatti strutturali, con particolare riguardo alle tematiche relative ai conflitti di interesse;

– prodotti da commercializzare e contrattualistica.

La funzione di Revisione Interna è responsabile della validazione relativamente alla coerenza con il sistema dei controlli e con le strategie aziendali.

gestione anomalie di conformità: il processo ha l'obiettivo di far pervenire alla funzione di Compliance flussi informativi su eventi critici ovvero situazioni rilevanti in termini carenze strutturali di conformità.

Le funzioni sottoelencate segnalano alla funzione di Compliance le situazioni di rilevanti carenze ed anomalie di conformità emerse nei modelli organizzativi in uso, nell'operatività aziendale, nell'ordinaria esecuzione dei controlli interni ed esterni ai processi:

- funzioni di Revisione Interna;
- funzioni con responsabilità ordinarie dei controlli esterni ai processi (controlli di secondo livello).

La funzione di Compliance a fronte delle segnalazioni pervenute, provvede all'integrazione del piano di mitigazione ed all'attivazione tempestiva delle fasi di implementazione.

informativa verso gli organi di vertice: il processo ha l'obiettivo di produrre informative e rendicontazioni verso gli Organi di Vertice al fine di consentire l'espletamento delle responsabilità loro assegnate in tema di gestione del rischio di non conformità. Per ciò che concerne la prestazione dei servizi di investimento il processo è finalizzato anche all'adempimento degli obblighi di Vigilanza.

In particolare la funzione di Compliance assicura i seguenti flussi informativi:

- segnalazioni di non conformità, riguardanti casi rilevanti di violazione delle norme e di non conformità dei modelli organizzativi in essere che possano comportare un alto rischio di sanzioni regolamentari o legali, perdite finanziarie di rilievo o danno di reputazione. L'informativa è trasmessa al Direttore Generale e agli Organi di Controllo aziendali;

- rendicontazione periodica, riguardante la valutazione sullo stato di conformità ed il piano degli interventi di mitigazione individuati. La relazione ed il piano vengono predisposti con cadenza almeno annuale e trasmessi al Direttore Generale e al Consiglio di Amministrazione previo esame degli Organi di Controllo aziendali;
- relazioni dovute ai sensi dell'art.16, comma 3 de l Regolamento congiunto Consob-Bankit, sulla base dei flussi ricevuti dalla funzione di Revisione Interna, al Direttore Generale e al Consiglio di Amministrazione previo esame degli Organi di Controllo aziendali (Collegio Sindacale e Comitato per il Controllo Interno).

comunicazione e formazione: il processo ha l'obiettivo di sensibilizzare sia dal punto di vista individuale che collettivo la cultura di Compliance ed il tema della conformità alla normativa (interna ed esterna), diffondendo la conoscenza delle politiche di Compliance, sviluppando competenze e professionalità necessarie a garantire la conformità e l'attuazione delle politiche di gestione del rischio in tutte le fasi dei processi aziendali, attraverso un processo di comunicazione continuo e strutturato a tutti i livelli dell'organizzazione aziendale. La funzione di Compliance verifica periodicamente il livello di sensibilità e di conoscenza sia individuale che collettivo nei confronti delle problematiche di conformità, anche attraverso il supporto della funzione Risorse Umane (Formazione).

A fronte dei gap emersi la funzione di Compliance, in accordo con la funzione Risorse Umane, definisce le azioni correttive in termini di interventi di formazione da erogare e comunicazione da veicolare alle strutture.

supporto ed assistenza: il processo ha l'obiettivo di erogare assistenza in via continuativa alle strutture aziendali e agli Organi di Vertice nelle

materie e nei processi aziendali in cui assume rilievo il rischio di non conformità.

Le funzioni coinvolte nel processo di Compliance forniscono consulenza alle strutture aziendali sull'applicazione di norme, codici di comportamento anche ai fini de gli adempimenti degli obblighi nella prestazione dei servizi di investimento e delle attività di intermediazione.

Per la funzione di Compliance, in particolare, è previsto:

- il supporto agli Organi di Vertice nella valutazione ex-ante della conformità alla regolamentazione applicabile nel caso di progetti innovativi e di ingresso nei nuovi mercati ed aree di business;
- il supporto agli Organi di Vertice nella verifica della coerenza del sistema premiante aziendale (in particolare retribuzione e incentivazione del personale) con gli obiettivi di rispetto delle norme, dello statuto nonché di eventuali codici etici o altri standard di condotta interni;
- la partecipazione ai processi di validazione di prodotti e servizi al fine di verificare la conformità degli stessi rispetto alle normative presidiate anche attraverso l'analisi preliminare degli standard documentali di offerta e della relativa contrattualistica;
- la tenuta dei rapporti con le Autorità di Vigilanza per le attività di cambiamento strutturale (pareri, consultazioni, partecipazione a gruppi di lavoro, …), coordinandosi con la funzione di Revisione Interna per i rapporti e le comunicazioni con gli Organi di Vigilanza.

revisione interna: il processo ha l'obiettivo di verificare periodicamente l'adeguatezza e la funzionalità della funzione di Compliance quale componente del complessivo sistema dei controlli.

La Funzione di Revisione Interna:

- accerta periodicamente la conformità, adeguatezza, efficienza ed efficacia del processo e della funzione di Compliance;
- segnala alle competenti funzioni, sulla base degli esiti delle verifiche effettuate, le eventuali azioni correttive da intraprendere;
- invia periodiche ed adeguate informative al Consiglio di Amministrazione, alla Direzione Generale, al Comitato per il Controllo Interno ed al Collegio Sindacale della Capogruppo circa l'attività di revisione svolta.

5 CONCLUSIONI

Ben oltre la complessità operativa interna di ogni intermediario, ulteriori fattori di complessità e di soggettività interpretativa da parte delle aziende, in merito allo svolgimento della funzione di verifica della conformità sono introdotti dalla proliferazione normativa che caratterizza il contesto attuale e dall'assenza, per il momento, di un chiaro e concreto coordinamento normativo (leggi e regolamenti spesso emanati in contesti differenti e rispondenti a differenti obiettivi).

Attraverso lo studio di alcune delle discipline che coinvolgono l'attività di compliance e di internal audit, è stato possibile individuare una comune linea di demarcazione che distingue le due funzioni e ne definisce le rispettive competenze, sia in tema di prestazione di consulenza, sia in tema di attività di attestazione delle procedure aziendali, che di verifica.

In alcuni casi, seppure in maniera non sempre così netta, è stato possibile individuare delle differenze nella "natura dei controlli" effettuati dall'organo di compliance e dalla Revisione Interna, che portano a chiarire le difformità fra una attività di consulenza finalizzata all'interpretazione di specifici processi operativi aziendali nell'ambito delle normative applicabili (funzione di verifica della conformità) e la prestazione di servizi di sostegno e assistenza intesi a fornire valore aggiunto e migliorare i complessivi processi di governance, risk management e controllo dell'intera organizzazione, senza assumerne responsabilità manageriali (funzioni di auditing). In questi termini, mentre l'attività di compliance risulta essere per sua stessa natura un servizio obbligatorio, connaturato con il ruolo preventivo della funzione, quella di Revisione Interna si caratterizza per essere una attività di consulenza "a chiamata", o su iniziativa della medesima funzione, focalizzata sulla necessità che il progetto/processo

risulti coerente con le attività di business e con il generale obiettivo di contenimento dei rischi aziendali considerati nel loro complesso.

In altri termini, mentre l'oggetto dell'attività di consulenza riguarda, nel caso della Funzione compliance, la legittimità stessa delle procedure aziendali e può essere sviluppata con il sostegno della Funzione Legale; la consulenza prestata dalla Revisione Interna è svolta sulle varie operazioni al fine di garantire la coerenza dell'operatività dell'azienda nell'ambito del sistema delle strategie d'impresa.

L'attività consultiva della funzione di compliance è svolta ex-ante, in fase di attuazione dei presidi, tenuto conto, ancora una volta, del ruolo preventivo della funzione stessa; ma anche ex-post, in fase di monitoraggio dei processi o quando si siano manifestate, o siano state segnalate dall'audit, carenze nei processi o nelle procedure, al fine di colmare i gap emersi. Le due funzioni sono chiamate, come visto in precedenza, a prestare attività di assurance dei processi e delle procedure aziendali; ma anche in questo contesto possono essere individuate delle differenze fra le attività svolte da ognuna di esse.

L'attività di assurance può riguardare l'assetto organizzativo, il sistema delle deleghe e dei poteri, il sistema dei controlli interni, i processi e le procedure aziendali, nonché le attività di reporting interno e di informativa alla clientela. In merito a questi aspetti, la Funzione compliance fornisce attività di assurance garantendo la corretta applicazione delle norme nei diversi momenti che interessano la vita aziendale; mentre la Funzione di auditing interno valuta obiettivamente ognuno di questi elementi, al fine di apprestare un giudizio indipendente in merito alla loro pertinenza ai requisiti previsti per il buon funzionamento della azienda stessa.

Infine, riguardo all'attività di verifica, la Funzione compliance opera un monitoraggio sulle procedure e sui processi, nonché sulle singole

operazioni o prodotti, conformemente all'obiettivo di individuare i possibili rischi di non-conformità; mentre la Revisione Interna è chiamata a verificare il corretto funzionamento del sistema dei controlli interni e dei meccanismi di gestione dei rischi nel loro complesso (rischi strategici, operativi, di credito, di mercato, reputazionale e di non conformità, altri rischi), al fine di individuare eventuali carenze e, ove necessario, predisporre adeguate soluzioni organizzative attraverso la consulenza ai vertici aziendali.

In altri termini, la Funzione compliance effettua verifiche analitiche, anche attraverso processi di risk-assessment, sviluppate direttamente dalla Funzione stessa, oppure dalle diverse unità operative coinvolte, in base a disposizioni dettate e validate dalla Compliance. Questa funzione rientra, dunque, a pieno titolo nell'attività di controllo di secondo livello.

Alla Revisione Interna, al contrario, è richiesta la padronanza dell'intero sistema di business e dei controlli interni, la sua attività di supervisione è svolta prevalentemente a distanza, ma anche attraverso visite ispettive in loco (nell'ottica della vecchia funzione di ispettorato) con specifico riferimento alle aree giudicate più rischiose a seguito dei risultati rivenienti da processi valutativi e di scoring, basati su indicatori di anomalia, emersi sia dalle analisi dirette, che dalla rielaborazione delle informazioni ricevute dai livelli di controllo sottostanti (controlli di linea, risk management, compliance).

L'attività di verifica svolta dalla Funzione compliance può essere idealmente suddivisa in due fasi: le verifiche che potremmo definire ordinarie, e le verifiche cosiddette straordinarie.

Le prime consistono nell'esame del funzionamento dei controlli di primo livello, in base alle procedure individuate dalla Compliance stessa, in fase di assurance e consulenza; tale attività viene condotta attraverso un

adeguato e sistematico processo di reporting periodico o eccezionale, quando si ravvisano situazioni di particolare rischiosità. Pertanto, le verifiche di pertinenza della Funzione di compliance, in linea di principio, dovranno riguardare l'esistenza, l'adeguatezza e il rispetto di presidi organizzativi presso le strutture operative, al fine di verificare che questi presidi siano organizzati e funzionino correttamente.

Le verifiche straordinarie sono, invece, richieste su materie specifiche (quali l'attività in titoli dei dipendenti della banca, la gestione dei conflitti d'interesse, l'antiriciclaggio o altri rischi ritenuti imprescindibili da ogni azienda) o in condizioni di particolare rilevanza di volta in volta individuate dalla banca e riportate nel relativo mandato. In questi casi, la Compliance può svolgere anche verifiche dirette sul campo; va da sé che la capacità di budget e le risorse umane dedicate dovranno essere adeguate all'ampiezza e alla complessità di queste esigenze straordinarie.

Per le proprie verifiche, sia "ordinarie" che "straordinarie", peraltro, la Funzione di compliance potrebbe avvalersi delle risorse professionali della struttura della Revisione Interna, purché questo avvenga sulla base di un rapporto chiaro e possibilmente formalizzato, che preveda comunque la valutazione finale delle risultanze emerse a carico della Funzione di compliance.

E' auspicabile che lo spirito di collaborazione che anima le due funzioni raggiunga il suo massimo grado di intensità nell'attività di verifica, affinché si possa evitare la duplicazione di attività ed elevare il grado di efficacia ed efficienza per la società.

Dunque, laddove si configuri un sistema di controlli integrato e incardinato gerarchicamente, sviluppato su diversi livelli, gestiti da organismi autonomi e dotati di autorevolezza e delle necessarie risorse umane e materiali, è possibile strutturare un processo efficace e privo di inutili duplicazioni di

costi, finalizzato al perseguimento dell'obiettivo della diffusione di una cultura del controllo e della conformità, mediante la collaborazione attiva fra le diverse funzioni coinvolte.

FUNZIONE DI COMPLIANCE	FUNZIONE DI REVISIONE INTERNA
•**OBIETTIVI** •Identificazione rischi di compliance •Processi conformi a norme e regole •**METODO** •Visione analitica dei rischi •**INTERVENTO** •*Bottom up*: analisi di tutti i processi esposti ai rischi di compliance	•**OBIETTIVI** •Valutazione del Sistema di Controllo Interno •Processi più efficienti ed efficaci •**METODO** •Visione sintetica dei rischi •**INTERVENTO** •*Top Down*: approfondimento di aree a rischiosità elevata

A tal fine è necessario che le relative competenze siano espressamente definite in un documento dal quale traspaiano anche le connesse responsabilità.

L'analisi fin qui esposta ha messo in evidenza come si presentino diversi elementi di incertezza e momenti di apparente sovrapposizione fra più funzioni chiamate a svolgere compiti molto prossimi fra loro.

Tuttavia, la linea espressa dalla Banca d'Italia nel documento di recepimento della nuova regolamentazione prudenziale internazionale, riguardo al metodo dei rating interni per il rischio di credito, e individuata, in maniera analoga, dalla direttiva MiFID, con la quale si introduce un'articolazione dei sistema dei controlli su tre livelli, sembra poter essere utilmente accolta e portarci alla considerazione che, quando saranno stati superati i limiti operativi di coordinamento fra le varie disposizioni e le diverse attività degli organismi aziendali, sarà possibile escludere la possibilità di sovrapposizione fra l'attività di revisione interna e quella di

compliance e intraprendere un processo di effettiva generazione del valore per tutta l'azienda.

E' necessario, in conclusione, che sia fatta chiarezza su un elemento di basilare rilevanza al fine di poter attribuire ruoli e competenze specifiche alla due funzioni: la Compliance è l'organo posto a presidio del rischio di non conformità, ma essa non assume responsabilità dirette riguardo ai possibili danni o alle sanzioni che possano generarsi a seguito del verificarsi di un evento attinente la compliance; questa responsabilità attiene alle unità di business che hanno generato il danno; pertanto, il controllo operativo è di competenza delle dirette unità di business, così come indicato dalla Banca d'Italia nel cosiddetto primo livello di controllo.

La Funzione di compliance è, invece, responsabile della coerenza del proprio operato ai principi di conformità; responsabili, altresì, della supervisione complessiva del sistema di gestione del rischio di non conformità alle norme sono il Consiglio di Amministrazione e il Collegio Sindacale. In questo contesto, la Revisione Interna non riveste un'attività limitata alla verifica della conformità, ma piuttosto alla valutazione della coerenza dei processi di controllo, di gestione dei rischi e di corporate governance.

Ciò detto, mentre la Revisione Interna deve accertare anche i comportamenti del personale impiegato nell'attività di business, la Compliance opera solo sulla verifica della coerenza dei processi e delle procedure aziendali ai requisiti di conformità alle norme che sono inserite nel suo perimetro di competenza, mentre le verifiche specifiche sui comportamenti riguardano solo alcune normative che le saranno state attribuite dal mandato. Del resto, se la Funzione di Compliance dovesse intervenire anche sui comportamenti, necessiterebbe di un impressionate numero di personale e correrebbe il rischio di sovrapporsi all'attività della

Revisione Interna, mentre, la scelta in prevalenza adottata dalle banche è quella di prevedere questo tipo di verifiche solo per quei comportamenti a forte impatto potenziale sui rischi reputazionali o di immagine dell'azienda[66].

Riguardo a un altro aspetto particolarmente controverso, più volte si è fatto riferimento al controllo esercitato dalla Revisione Interna sulla Compliance e ci si è chiesto se la compliance debba verificare sulla conformità dell'attività svolta dalla Revisione Interna stessa.

Pare plausibile ritenere che, pur non rientrando fra le sue immediate competenze, in ogni modo, la Funzione di Compliance abbia il dovere morale di denunciare possibili comportamenti non conformi alle norme da parte dell'audit, essendo essa, comunque, una funzione indipendente, che riferisce direttamente all'alta direzione.

E' auspicabile, pertanto, che le due funzioni, pur mantenendo competenze e responsabilità distinte, riconoscano il dovere di effettuare reciproci scambi di informazioni, e di rilevare, in ogni caso, quando si renda necessario, le eventuali carenze nell'operato dell'una o dell'altra.

Una precisazione è, infine, doverosa, riguardo alla distinzione esistente fra "attività di compliance" e "funzione di compliance"; perché il rischio di non conformità è un rischio trasversale, che coinvolge tutti i livelli dell'attività bancaria, pertanto nessuna attività e nessuna unità operativa può dirsi immune da tale eventualità e pertanto indifferente alla compliance.

[66] Si fa notare che la gran parte delle realtà internazionali prevede già da tempo una forte componente di "controllo permanente" per la Funzione di compliance, la quale, partecipa a tutte le attività delle banca fin dalla definizione strategica. La tripartizione dei livelli di controllo tipica delle realtà italiane, invece limita l'operato della Funzione di conformità al cosiddetto secondo livello dei controlli; prevedendo la possibilità di intervenire a tutto tondo solo per quella tematiche che le siano state attribuite da mandato, perchè ritenute avere un forte impatto sui rischi di compliance e reputazionale.

I compiti e le responsabilità attribuite alla funzione compliance, nell'ambito di un articolato sistema di controlli interni e di una attività, quella bancaria, complessa e multiprodotto, non possono che essere circoscritti e ben definiti in strumenti formali e oggettivi, che descrivano attentamente i ruoli e le responsabilità del compliance officer, con specifico riferimento in particolare a quelle funzioni che possono presentare sovrapposizioni inutilmente costose ed inefficienti.

Questo processo non può che essere frutto di una policy interna alle banche e agli altri intermediari finanziari, in accordo con le caratteristiche peculiari di ognuno di essi, in termini dimensionali, di attività svolta, di complessità operativa e organizzativa; ma resta inteso che il rischio di compliance coinvolge e interessa tutti i livelli dell'organizzazione aziendale.

Dall'esame dell'impianto del Sistema dei Controlli Interni analizzato nel caso della "Nostra Banca" le considerazioni sopra espresse trovano piena applicazione nella realtà operativa vigente presso l'intermediario su cui è stato effettuato il focus operativo.

Infatti le due Funzioni, Compliance e Revisione Interna, sono risultate caratterizzate dall'indipendenza necessaria allo svolgimento delle attività previste dalle loro mission aziendali.

Il perimetro di azione è comune a entrambi le Funzioni, ovvero tutto l'ambito aziendale e tutte le fonti informative connesse con l'attività di business svolta dalla "Nostra Banca". Nel caso della Compliance è prevista un'attività di controllo relativa alla conformità dei processi che vengono messi a disposizione della macchina operativa, attività strettamente connessa alle "reazioni" dell'azienda a tutte le variazioni, numerosissime, del contesto normativo che regola la prestazione dei servizi bancari e finanziari.

Invece, la Revisione Interna svolge un'attività di controllo sull'operatività svolta quotidianamente dall'azienda, e che risulti conforme alle policy aziendali e coerente con le norme che regolano a livello nazionale che regolano le materie di impatto dell'attività aziendale. Non da ultimo, la sua responsabilità primaria resta quella sul monitoraggio del complessivo Sistema dei controlli Interni.

Nello specifico se analizziamo sia l'attività di consulenza che l'attività di assurance esplicata da entrambe le funzioni, sui medesimi ambiti, si riescono a individuare in maniera lineare i compiti "distinti" dalle due funzioni che però non possono assolutamente prescindere dall'istituzione di un flusso continuo di reportistica e informative tra le due funzioni facenti parte del medesimo sistema dei controlli interni.

Di seguito, sia sulla base di quanto esaminato e rielaborato nell'ambito della letteratura e nella dottrina in materia nel corpo della presente tesi di laurea sia sulla base delle considerazioni emerse dall'analisi del caso pratico della "Nostra Banca", si fornisce un parallelo delle specifiche attività svolte dalle due funzioni, su assurance e consulenza, da cui si evince la necessità di un "legame informativo" forte finalizzato alla massimizzazione dell'efficacia e dell'efficienza del sistema dei controlli interni nonché dal conseguimento di un soddisfacente livello di economicità delle attività di controllo realizzate dalla Funzione di Compliance e dalla Funzione di Revisione Interna.

Per ciò che concerne invece l'attività di consulenza la Revisione Interna la finalizza prevalentemente mediante la proposta di soluzioni idonee a garantire il superamento dei punti di debolezza del Sistema dei Controlli Interni. La sua attività si esplica sia nel momento in cui emergono disallineamenti tra il Sistema dei Controlli Interni e il modello di business e di governo adottato dall'azienda, sia nella fase di impianto/revisione di

processi e procedure, con l'obiettivo di garantire coerenza e linearità all'intero impianto dei controlli a presidio dei rischi. Per la Funzione di Compliance, l'oggetto dell'attività di Consulenza, riguardando la rispondenza dei processi ai dettami normativi, ai principi e ai valori promossi dall'azienda, è rappresentato dalla legittimità stessa delle procedure aziendali.

In relazione all'attività di assurance, entrambi le funzioni operano nell'ambito:

dell'assetto organizzativo: la Revisione Interna valuta l'adeguatezza dell'assetto organizzativo relativamente ai requisiti previsti per il "buon funzionamento" della macchina aziendale; la Funzione di Compliance ne verifica la conformità rispetto alla normativa di riferimento, con l'obiettivo, in particolare, di presidiare il conflitto di interessi eventualmente emergente nei compiti attribuiti alle singole unità organizzative.

sistema delle deleghe e dei poteri: la Revisione Interna valuta la corrispondenza del sistema delle deleghe e poteri rispetto a quanto statuito dalle specifiche delibere del Consiglio di Amministrazione ovvero dalle direttive aziendali e verifica che la distribuzione dei ruoli e delle responsabilità non determini duplicazioni, sovrapposizioni od omissioni di compiti. La Funzione di Compliance deve valutare che l'allocazione delle deleghe e dei poteri garantisca l'esercizio delle responsabilità attribuite dalle normative di riferimento a specifici soggetti/funzioni aziendali nonché un idoneo presidio dei conflitti di interesse, sia riferiti alle risorse all'interno delle diverse unità organizzative, sia in relazione ai singoli esponenti aziendali.

sistema dei controlli interni: la Revisione Interna analizza l'adeguatezza del sistema stesso, relazionando periodicamente l'Alta Direzione e gli Organi Societari sugli esiti delle attività svolte e proponendo soluzioni di

miglioramento; a tal fine provvede a valutare il funzionamento di tutti gli attori del Sistema dei Controlli Interni, tra cui la Funzione di Compliance. La Funzione di Compliance ha il compito di effettuare e aggiornare periodicamente la mappatura dei rischi di non conformità e reputazionali emergenti dai processi/prodotti, con stretto riferimento all'evoluzione del modello di business aziendale, all'introduzione di nuove normative e all'aggiornamento di quelle vigenti, nonché all'adozione di norme di autoregolamentazione e di codici di condotta.

modelli di gestione del rischio: l'attività di Assurance della Revisione Interna si focalizza su tutti i modelli di gestione del rischio adottati dall'azienda allo scopo di verificarne il corretto ed efficace funzionamento, ivi incluso quello di Compliance, con lo scopo di assicurare che quanto adottato consenta al management un'efficace gestione dei rischi. La Funzione di Compliance progetta e provvede all'aggiornamento del modello di gestione del rischio relativo ai rischi di non conformità e reputazionali, adottato coerentemente con le strategie e l'operatività aziendale. La Funzione di Compliance valuta, inoltre, l'aderenza alla normativa, anche degli altri modelli di gestione dei rischi adottati dalla società.

processi e procedure aziendali: l'attività di Assurance svolta dalla Revisione Interna è sistematicamente rivolta al miglioramento dell'efficacia e dell'efficienza dell'organizzazione attraverso la valutazione dei processi aziendali. Obiettivo di tale attività è fornire al management una valutazione di affidabilità sul Sistema di Controllo. La Funzione di Compliance identifica costantemente le norme applicabili, ne valuta la loro integrazione nei processi e procedure aziendali, garantendone la corretta applicazione e valutandone l'impatto. La Funzione di Compliance svolge tale attività di Assurance nel continuo". Relativamente alla procedure aziendali la Revisione Interna svolge un ruolo attivo nelle fasi di disegno delle

procedure aziendali, fornendo expertise nell'applicazione dei principi di controllo e nell'analisi dei processi e dei rischi (ma in base agli Standard Professionali non può essere chiamato alla redazione delle procedure aziendali, ndr). Inoltre, a seguito di interventi di verifica, la funzione può raccomandare azioni di miglioramento sui presidi di controllo formalizzati nelle procedure aziendali". La Funzione di Compliance, invece, garantisce che le procedure organizzative contengano i presidi necessari a prevenire la violazione di norme di eteroregolamentazione ed autoregolamentazione".

sistemi aziendali di reporting e informativa: la Funzione di Revisione Interna valuta il livello di adeguatezza dei sistemi informativi aziendali e l'affidabilità delle informazioni disponibili rispetto alla complessità del contesto operativo, alla dimensione e all'articolazione territoriale dell'impresa" e "verifica l'adeguatezza dei presidi organizzativi adottati dalla società per la sicurezza fisica, logica e organizzativa del sistema informativo aziendale". La Funzione di Compliance valuta la conformità del reporting e dell'informativa aziendale con riferimento alla sua idoneità a rispondere ai requisiti normativi vigenti o alle disposizioni interne stabilite dall'azienda, anche in termini di contenuti e tempistica, identifica le norme applicabili alla società e si assicura del corretto recepimento delle stesse nelle procedure aziendali di reporting e di produzione dell'informativa.

attività di controllo e verifica: la Funzione di Revisione Interna esplica le proprie attività di verifica "mediante specifici interventi sul sistema dei controlli, mirati a valutare la rischiosità intrinseca di particolari aree di attività. La Funzione di Compliance è chiamata invece a svolgere attività di monitoraggio nel continuo sui presidi esistenti nei processi e nelle procedure di mitigazione dei rischi di non conformità e reputazionali".

6 BIBLIOGRAFIA

ABI, Libro Bianco sulla Funzione Compliance. Coordinamento scientifico di A. Alberici, M. Anolli, A. Carretta, M. Decastri, M. Di Antonio, M. Lamandini, P. Schwizer, Bancaria Editrice, Roma 2008.

ABI, Linee guida dell'Associazione Bancaria Italiana per l'adozione di modelli organizzativi sulla responsabilità amministrativa delle banche (d.lgs n. 231/2001), 2004,

AIIA – AICOM, Le Funzioni di Internal Audit e di Compliance: ruoli, responsabilità e ambiti di rispettiva competenza, 2008,

M. ANOLLI – F. RAJOLA, Il rischio di reputazione e di non conformità. strumenti e metodi per la governance e la gestione operativa, Bancaria Editrice, Roma 2010.

ALFON I., ANDREWS P. (1999), Cost-Benefit Analysis in Financial Regulation – how to do it and how it adds value, FSA Occasional Paper Series, n. 3, settembre.

AMERICAN BANKING ASSOCIATION (ABA) (2003), Compliance Watch 2003, The Nationwide Bank Compliance Officer Survey, ABA Banking Journal, giugno.

ASSOCIAZIONE BANCARIA ITALIANA (ABI) (1999), Sistemi di Controllo Interno ed evoluzione dell'Internal Auditing, Area Studi e Tecnologie, aprile.

ASSOCIAZIONE BANCARIA ITALIANA (ABI) (2004a), Position paper del sistema bancario italiano sul documento del Comitato di Basilea "The compliance function in banks", gennaio.

ASSOCIAZIONE BANCARIA ITALIANA (ABI) (2004b) Linee guida dell'Associazione bancaria Italiana per l'adozione di modelli organizzativi sulla responsabilità amministrativa delle banche (d.lgs. n. 231/2001), febbraio.

ASSOCIAZIONE ITALIANA INTERNAL AUDITORS (IIA) (2005), Standard Internazionali e Guide Interpretative per la Pratica Professionale dell'Internal Auditing, settembre

ANTHONY R. N., HAWKINS D. F., MERCHANT K. A., MACRÌ D. M. (2004), Sistemi di controllo. Analisi economiche per le decisioni aziendali, seconda edizione, McGraw Hill.

BANCA D'ITALIA (1999), Istruzioni di vigilanza per le banche.

BANCA D'ITALIA (2006), Normativa di vigilanza in materia di "conformità alle norme (compliance)", Documento di consultazione, agosto.

BANCA D'ITALIA (2006b), Recepimento della nuova regolamentazione prudenziale internazionale Metodo dei rating interni per il calcolo del requisito patrimoniale a fronte del rischio di credito, Documento di consultazione, luglio BANCA D'ITALIA (2006c), Recepimento della nuova regolamentazione prudenziale internazionale - rischi operativi (metodi avanzati - ama), Documento di consultazione, luglio.

BARAVELLI M., VIGANO' A. (a cura di) (2000), L'Internal Audit nelle banche, Bancaria Editrice, Roma.

BASEL COMMITTEE ON BANKING SUPERVISION, (2006), International Convergence of Capital Measurement and Capital Standards - A Revised Framework Comprehensive Version, June.

G. CAROSIO, La Funzione di Compliance tra Basilea II e MiFID, intervento al III Incontro Compliance "Strategies, governance, compliance: le sfide della direttiva MiFID e l'integrazione del mercato finanziario europeo", organizzato da AICOM e Dexia Crediop, Roma 21 settembre 2007,

CAROSIO G. (1990), Problems of harmonization of the regulation of financial intermediation in the european community, in "European Economic Review", n. 34, pp.578-586.

CARRETTA A. (a cura di) (1998), Banche e intermediari non bancari: concorrenza e regolamentazione, Bancaria Editrice, Roma.

CARRETTA A., SCHWIZER P. (2004), La vigilanza bancaria dopo I controlli interni: verso la consulenza regolamentare e il Knowledge management, Bancaria n. 2.

CARRETTA A., SCHWIZER P., STEFANELLI V., (2003), Oltre la regolamentazione: il sistema dei controlli interni degli intermediari

finanziari. Cultura del controllo o controllo della cultura?, Ottavo Rapporto Fondazione Roselli, Edibank, Milano.

CARRETTA A. (2006), Compliance e cultura bancaria, Intervento al Convegno "Etica e regole nella finanza. La funzione compliance", Università dagli Studi di Roma "Tor Vergata" e Fondazione "Gabriele Berionne", Roma, 5 Dicembre.

CEBS (2006), Guidelines on the Application of the Supervisory Review Process under the Pillar 2, gennaio.

CETIF (2007), Riflessi organizzativi della compliance nelle banche. Sintesi del rapporto di ricerca, in www.cetif.it.

CLEMENTE C. (2006), Vigilanza sugli enti creditizi, Banca d'Italia, La funzione di compliance nelle banche italiane: evoluzione normativa e contributo alla creazione del valore, intervento al II Incontro Compliance, AICOM, 28 giugno, Roma.

COLA C. (2005), La compliance e il modello organizzativo, intervento presso l'Università di Roma Tre, 11 marzo.

COMANA M. (2005), Prefazione al testo "La compliance in banca" di Pogliaghi P. e Vandali W. (a cura di), Bancaria Editrice, Roma.

COMITATO DI BASILEA (2004), Convergenza internazionale della misurazione del capitale e dei coefficienti patrimoniali, Basilea, giugno 2004.

CICCHINÈ M. (2005), Funzione compliance: attività e indicatori di performance, intervento al Convegno ABI Formazione "Modelli, strumenti e benchmark per la funzione compliance", Roma, 25-26 ottobre.

D'ARCANGELIS S. (2006), La funzione "compliance" nelle banche: caratteristiche operative, in "Amministrazione e Finanza", n. 2.

HINNA L. (2006), La compliance per creare valore per la banca, gli stakeholder, i clienti ed il personale dell'azienda, intervento al Convegno "Compliance in banks: dalle regole al valore", Roma 16-17 ottobre.

HUTTER B., POWER M. (2000), Risk management and business regulation, in "Financial Times Mastering Risk Series".

KIRCHMAIER T., SELVAGGI M. (2006), The dark side of "good" corporate governance: compliance-fuelled book-cooking activities, FMG Discussion Paper, n. 559.

KPMG (2006), I risultati di una survey sulle funzioni di compliance delle banche italiane, intervento al Convegno "Compliance in banks: dalle regole al valore", Roma 16-17 ottobre.

PIZOLLI M. (2006), Organizzazione delle funzioni di controllo interno presso le banche ed i commercianti di valori mobiliari con particolare riferimento alla funzione di Compliance, Centro Studi Bancari, Associazione Bancaria Ticinese, Quaderni di ricerca, n. 25, ottobre.

POGLIAGHI P., ETTORI S. (2005), La funzione compliance nelle banche mediopiccole: come organizzarla e inquadrarla, in "Bancaria", n. 6.

POGLIAGHI P., VANDALI W. (2005) (a cura di), La compliance in banca, Bancaria Editrice, Roma

PROTIVITI (2006), Legge Risparmio & Informativa Societaria: Riflessi sul Sistema di Controllo Interno, in "Insight", n. 8, gennaio.

TREVINO L. K., WEAVER G. R., GIBSON D. G., TOFFLER B. L. (1999), Managing Ethics and Legal Compliance: What Works And What Hurts, in "California Management Review", Vol. 41, n. 2.

USELLI A. (2004), I rischi operativi nel contesto normativo e nelle evidenze della pratica operativa: l'esame di alcuni aspetti critici, Università dell'Insubria, Facoltà di Economia,

USELLI A. (2005), Conformità nella gestione dei rischi operativi, in Pogliaghi P., Vandali W. (a cura di) (2005), La compliance in banca, Bancaria Editrice, Roma.

WEAVER G. R., TREVINO L. K. (1999), Compliance and Value Oriented Ethics Programs: Influences on Employees' Attitudes and Behavior, in "Business Ethics Quarterly", Vol. 9, Issue 2.

WEAVER G. R., TREVINO L. K., COCHRAN P. L. (1999), Corporate Ethics Practices in the Mid-1990's: An Empirical Study of the Fortune 1000, in "Journal of Business Ethics", n. 18.

WEAVER G. R., TREVINO L. K. (2001), The rule of human resources in ethics/compliance management. A fairness perspective, in "Human Resource Management Review", vol. 11, issue 1/2.

WEAVER G. R., TREVINO L. K. (2001), Outcomes of Organizational Ethics Programs: Influences of Perceived Values, Compliance and Distrust Orientations, Academy of Management Best Papers Proceedings.

WEBER J., FORTUN D. (2005), Ethics and Compliance Officer Profile: Survey, Comparison and recommendations, in "Business and Society Review", vol. 110, issue 2, p. 97 – June.

ZAMAGNI S. (2006), Ruolo delle regole e dell'etica nell'attività finanziaria, Intervento al Convegno "Etica e regole nella finanza. La funzione compliance", Università dagli Studi di Roma "Tor Vergata" e Fondazione "Gabriele Berionne", Roma, 5 dicembre.

7 WEBSITES

www.complianceaziendale.com

www.bancaditalia.it

www.aicom.it

www.bancaditalia.it

www.isacaroma.it

www.ilsole24ore.it

www.assoaicom.org

www.repubblica.it

www.dirittobancario.it

www.emagazine.assonime.it

www.olm-cuoa.it

www.compliancenet.it

www.tidona.com

www.wikipedia.it